



JIM McDONNELL, SHERIFF

County of Los Angeles
Sheriff's Department Headquarters
4700 Ramona Boulevard
Monterey Park, California 91754-2169



A Tradition of Service

December 16, 2014

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
Los Angeles, California 90012

Dear Supervisors:

**APPROVAL OF AGREEMENT WITH NEC CORPORATION OF AMERICA FOR A
MULTIMODAL BIOMETRIC IDENTIFICATION SYSTEM SOLUTION
(ALL DISTRICTS) (3 VOTES)**

**CIO RECOMMENDATION: APPROVE (X) APPROVE WITH MODIFICATION ()
DISAPPROVE ()**

SUBJECT

The Los Angeles County (County) Sheriff's Department (Department) is requesting the Board's authorization to execute an Agreement with NEC Corporation of America (NEC), for the provision and maintenance of a Multimodal Biometric Identification System Solution (MBIS Solution) for the Department's Data Systems Bureau (DSB), acting as the lead agency in support of the multi-agency Los Angeles County Regional Identification System (LACRIS).

IT IS RECOMMENDED THAT THE BOARD:

1. Approve and instruct the Mayor of the Board to authorize the Sheriff to finalize and execute an Agreement, substantially similar to the attached Agreement, with NEC for a contract term commencing upon such execution and continuing for the initial term of six years from the County's final acceptance of the MBIS Solution, with an option to extend for an additional four-year period through the maximum term of ten years from the County's final acceptance of the MBIS Solution, and a Maximum Contract Sum of \$24,424,000 for the entire term of the Agreement.
2. Delegate authority to the Sheriff, or designee, to execute change notices and amendments, or modify the Agreement as set forth in the Agreement in order to: (1) add and/or update standard County contract provisions as required by the Board or the County's Chief Executive Office (CEO); (2) exercise the term extension option; (3) effectuate an assignment of rights and/or delegation of

duties pursuant to the Assignment and Delegation provision under the Agreement; (4) acquire goods or services related to the MBIS Solution using Pool Dollars allocated for the Agreement without increasing the Maximum Contract Sum allocated for the term of the Agreement with prior notice to the County's Chief Information Officer (CIO) and County Counsel; (5) amend the Agreement to reflect changes to sales/use tax as a result of any change in the applicable State of California (State) or other local law and to increase the Maximum Contract Sum under the Agreement accordingly; and (6) amend the Agreement to acquire additional workstations using Pool Dollars in the event of a substantial expansion of a law enforcement agency supported by the MBIS Solution, by increasing the amount of available Pool Dollars and the Maximum Contract Sum accordingly with prior notice to the CIO and County Counsel.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Under the proposed Agreement, NEC will provide the County with services to replace the existing Automated Fingerprint Identification System (AFIS) with the MBIS Solution. The MBIS Solution will provide law enforcement agencies throughout the County with regional fingerprint, facial, iris, and other biometric identification services that may become available during the term of the proposed Agreement. The MBIS Solution will interface with and access the State Department of Justice's AFIS, and the Federal Bureau of Investigation's Next Generation Identification System to search fingerprint, facial, and iris image data. The MBIS Solution will provide timely identification of persons arrested by law enforcement agencies throughout the County, and provide suspect information for latent fingerprint images found at crime scenes.

The MBIS Solution will incorporate emerging technologies to provide powerful new tools to crime investigators. The speed, accuracy, and functionality of the MBIS Solution will enhance fingerprint examiners' ability to identify criminals and elevate public safety. The Agreement provides for metrics to measure the accuracy, speed, and functionality of the MBIS Solution, all of which will be tested prior to implementation and throughout the term of the Agreement.

The Department is the proprietor of LACRIS, which provides criminal identification services to the Department, Los Angeles Police Department, and other local law enforcement agencies within the County. The MBIS Solution will function as a critical component of LACRIS.

The MBIS Solution will receive and search electronically transmitted fingerprints, mugshots, and iris images in local databases, and provide law enforcement agencies with positive identifications of arrestees. The MBIS Solution will also allow investigators to process and identify fingerprint images obtained from crime scene.

Implementation of Strategic Plan Goals

The MBIS Solution supports the County's Strategic Plan, Goal 3, Integrated Services Delivery. The services provided by the MBIS Solution will adopt a "service bureau model" approach, relieving the Department of the traditional responsibility of making significant capital and human resource investments in equipment, software, and ongoing maintenance prior to the operation of the MBIS Solution. The "service bureau model" allows for the continual and optimal delivery of services to law enforcement agencies throughout the County, by providing fingerprint examiners, investigators and custodial officers with a continuously high level of system performance.

FISCAL IMPACT/FINANCING

The Maximum Contract Sum allocated for the term of the Agreement is \$24,424,000 which includes the following components:

- Service fees for the initial term of six years at \$2,090,400 per year, for a total of \$12,542,400 to be paid following the County's final acceptance of the MBIS Solution;
- Service fees for the four-year optional extended term at \$1,970,400 per year, for a total of \$7,881,600; and
- An allocation of Pool Dollars in the amount representing less than 20 percent of the service fees for procurement of the MBIS Solution related optional goods and/or services in the event of unforeseen emergencies or potential future service requirements, for a total of \$4 million for the maximum term of the Agreement.

The Remote Access Network Board has approved funding for this Agreement from the AFIS fund for the term of the Agreement, including the optional extension and the Pool Dollars for optional goods/services. There will be no Net County Costs incurred for the services provided by NEC.

No fees will be paid to NEC prior to the County's issuance of final acceptance of the MBIS Solution. All service fees will be paid quarterly in arrears.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The proposed Agreement will serve as a successor to Agreement Number 74083 with 3M Cogent, Incorporated (3M). To ensure successful completion of and transition to the MBIS Solution, the Agreement with 3M was extended by the Board on October 13, 2014, for up to three years. NEC is scheduled to provide implementation and transition services over a 24-month period, during which time, 3M's Agreement to provide continued maintenance and support of the legacy AFIS system will remain in full force and effect.

This Agreement with NEC will become effective upon the Board's execution and will continue for the initial term up to and through six years from the County's final acceptance of the MBIS Solution, with the extended optional term of four years, at the delegated discretion of the Sheriff.

The Agreement contains all County mandated provisions, including Time Off for Voting. In addition, NEC is required to notify the County when the Agreement term is within six months from expiration, and when payments have reached 75 percent of the authorized Maximum Contract Sum.

The Agreement also contains the information technology provisions applicable to the "service bureau model," Patrick Ogawa, Chief Deputy Executive Officer, Board of Supervisors including security requirements, remedies against NEC's deficient performance or breach of warranties, technology errors, omissions, and cyber insurance coverages, as well as intellectual property indemnification.

As a result of the negotiations, the County, with the concurrence from the CEO's Risk Management Branch, has agreed to limit NEC's general indemnification obligations to those resulting from negligent acts or omissions, with the liability of either party capped at \$12 million for the initial term of the Agreement and \$6 million for the optional extended term. Under the "service bureau payment model," NEC's cost of initial investment is incorporated into the service fees, which will be due only after the County's final acceptance of the MBIS Solution. In the event the County terminates the Agreement for convenience during the initial term, the County will reimburse NEC a prorated amount of its initial project investment cost, which will be based on the time of termination as provided in the Agreement. The Agreement also locks the prices for the acquisition of additional workstations in the event of an expansion of any agency supported by the MBIS Solution.

The CIO reviewed and recommends approval of this Agreement. The CEO's Risk Management Branch has reviewed and concurs with the provisions relating to insurance and indemnification.

County Counsel will approve the attached Agreement as to form.

CONTRACTING PROCESS

On July 30, 2013, the County's Information Systems Advisory Body (ISAB) issued a Request for Proposals (RFP) for the MBIS Solution developed with the assistance from a third-party independent consulting firm contracted by ISAB. In response to the RFP, ISAB received proposals from three qualified vendors by the September 27, 2013, due date.

The evaluation committee was comprised of subject matter experts from the County, as well as other local law enforcement agencies throughout the County. The committee independently reviewed and scored the proposals based on the predefined evaluation criteria in conformance with the Board's informed averaging guidelines. Areas of evaluation included technical discussion, management approach, experience, and capability with price being independently evaluated.

After completing the evaluation process, it was determined that NEC was the highest scoring qualified proposer.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

There will be no negative impact on current services.

CONCLUSION

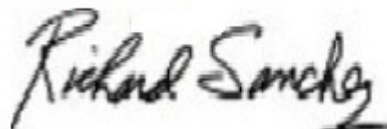
Upon Board approval, please instruct the Executive Officer-Clerk of the Board to return an adopted copy of the Board letter to the Department's Contracts Unit.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim McDonnell". The signature is stylized with a large, looping initial "J" and "M".

JIM McDONNELL
Sheriff

Reviewed by:

A handwritten signature in black ink, appearing to read "Richard Sanchez". The signature is written in a cursive style.

RICHARD SANCHEZ
Chief Information Officer

JM:AF:af



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

Office of the CIO
CIO Analysis

NUMBER:

CA 14-28

DATE:

10/10/2014

SUBJECT:

**APPROVAL OF AGREEMENT WITH NEC CORPORATION OF AMERICA FOR
A MULTIMODAL BIOMETRIC IDENTIFICATION SYSTEM SOLUTION**

RECOMMENDATION:

☒ Approve ☐ Approve with Modification ☐ Disapprove

CONTRACT TYPE:

☒ New Agreement ☐ Sole Source
☐ Amendment to Contract #: ☐ Other: Describe contract type.

CONTRACT COMPONENTS:

☒ Software ☐ Hardware
☐ Telecommunications ☒ Professional Services

SUMMARY:

Department Executive Sponsor: Sheriff Jim McDonnell

Description: Approve an Agreement with NEC Corporation of America (NEC) to provide the Los Angeles County Regional Identification System (LACRIS) of the Los Angeles County's (County) Sheriff's Department (Department) with acquisition, implementation, and maintenance of a new Multimodal Biometric Identification System (MBIS).

Contract Amount: **\$ 24,424,000** Funding Source: Automated Fingerprint Identification System (AFIS) Fund.

Approved by RAN (Remote Access Network)

☐ Legislative or Regulatory Mandate ☐ Subvened/Grant Funded:

**Strategic and
Business Analysis**

PROJECT GOALS AND OBJECTIVES:

This proposed Agreement will provide for the acquisition, implementation, and maintenance of a new MBIS, to be used by the Department, and other local law enforcement agencies, as part of their LACRIS.

BUSINESS DRIVERS:

The Department has an existing LACRIS Automated Fingerprint Identification System (LAFIS), provided by Cogent Information Systems, Inc., which will be replaced. The Cogent Agreement was extended until October 12, 2016, to have continuous support for the system until implementation of the new MBIS system. NEC will replace the 12-year old fingerprint identification system with a new state-of-the-art solution that will use fingerprint, facial, and iris capturing to fuse into one single identification system. LACRIS is managed by the Department, with oversight, direction, and funding authorization by the Remote Access Network (RAN) Board.

PROJECT ORGANIZATION:

The Department's LACRIS Unit will be driving this project with a Lieutenant assigned as the Local Cal-ID Project Manager, who will be managing the ongoing operation of this project. The Chief Information Office (CIO) recommended and supported hiring a dedicated technical manager, in which the Department received approval from RAN to hire an Information Technology Specialist I to lead the technical implementation of the project.

PERFORMANCE METRICS:

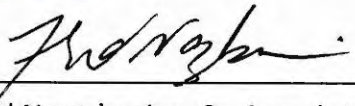

NEC will be responsible for all services, including: software application, personnel, back-up facilities, equipment, material, supplies, maintenance, support, and management required to perform all functions for MBIS. A comprehensive maintenance Service Level Agreement addresses : 24/7 coverage onsite/remote access, storage capacity with 2 percent annual growth; compliance with National Institute of Standards and Technology (NIST), archive of all input and output transactions through the term of the Agreement, 99.8 percent service availability and restoration, data back-up and recovery, technology refresh and enhancement, software updates, hardware upgrades, etc.

STRATEGIC AND BUSINESS ALIGNMENT:

This Agreement supports County Strategic Plan Goal 1, Operational Effectiveness, and Goal 2, Fiscal Sustainability.

PROJECT APPROACH:

A dedicated team and a project manager will be assigned to manage this project. A project control document will be developed during the first few weeks of engagement to identify the implementation phase and time line.

	<p>ALTERNATIVES ANALYZED:</p> <p>An RFP was issued, and after the evaluation process, NEC was determined to be the highest scoring, qualified proposer. The Department has invested over \$35 million, with the existing vendor with approximately \$1 million in annual maintenance cost. The new, fully hosted, and managed Agreement is more cost-effective, and will provide more value with the additional biometric options.</p>												
Technical Analysis	<p>ANALYSIS OF PROPOSED IT SOLUTION:</p> <p>The current LACRIS application and hardware requires upgrades. MBIS will include new technology, finger/palm prints, face, and iris capturing capabilities. The hosted services will include disaster recovery and back up data centers.</p> <p>The project implementation is expected to take 18 months. The goal of this new technology is to replace the existing legacy system and leverage the latest technology in order to provide a modern, supported system that will enhance mission-critical operations over the next ten years.</p>												
Financial Analysis	<p>BUDGET:</p> <table> <tr> <td>Contract costs:</td><td></td></tr> <tr> <td> Services</td><td>\$20,424,000</td></tr> <tr> <td> Contingency.....</td><td>\$ 4,000,000</td></tr> <tr> <td>Ongoing annual costs:</td><td>\$2,090,400 x first 6 years = \$12,542,400</td></tr> <tr> <td></td><td>\$1,970,400 x ext. 4 years = \$ 7,881,600</td></tr> <tr> <td>Total Agreement Costs:</td><td>\$ 24,424,000</td></tr> </table>	Contract costs:		Services	\$20,424,000	Contingency.....	\$ 4,000,000	Ongoing annual costs:	\$2,090,400 x first 6 years = \$12,542,400		\$1,970,400 x ext. 4 years = \$ 7,881,600	Total Agreement Costs:	\$ 24,424,000
Contract costs:													
Services	\$20,424,000												
Contingency.....	\$ 4,000,000												
Ongoing annual costs:	\$2,090,400 x first 6 years = \$12,542,400												
	\$1,970,400 x ext. 4 years = \$ 7,881,600												
Total Agreement Costs:	\$ 24,424,000												
Risk Analysis	<p>RISK MITIGATION:</p> <p>There are minimal risks to this proposed implementation. The existing fingerprint images follow the National Institute of Technology (NIST) standards which will simplify conversion.</p> <p>The Chief Information Security Officer (CISO) reviewed the Agreement and did not identify any IT security or privacy related issues.</p>												
CIO Approval	<p>PREPARED BY:</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="text-align: center;">  Fred Nazarbegian, Sr. Associate CIO </div> <div style="text-align: center;"> <u>11-26-14</u> Date </div> </div> <p>APPROVED:</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="text-align: center;">  Richard Sanchez, County Chief Information Officer </div> <div style="text-align: center;"> <u>11-26-14</u> Date </div> </div>												

**LOS ANGELES COUNTY
SHERIFF'S DEPARTMENT**



**AGREEMENT
BY AND BETWEEN
COUNTY OF LOS ANGELES
AND
NEC CORPORATION OF AMERICA
FOR
MBIS SOLUTION**

DECEMBER 2014

TABLE OF CONTENTS

1.	APPLICABLE DOCUMENTS	1
1.1	INTERPRETATION	1
1.2	ENTIRE AGREEMENT	2
1.3	DEFINITIONS	2
2.	ADMINISTRATION OF AGREEMENT – COUNTY	18
2.1	COUNTY ADMINISTRATION	18
2.2	COUNTY KEY PERSONNEL	19
2.3	COUNTY PERSONNEL	19
2.4	APPROVAL OF WORK	19
3.	ADMINISTRATION OF AGREEMENT – CONTRACTOR	19
3.1	CONTRACTOR ADMINISTRATION	19
3.2	CONTRACTOR KEY PERSONNEL	20
3.3	APPROVAL OF CONTRACTOR’S STAFF	20
3.4	BACKGROUND AND SECURITY INVESTIGATIONS	21
3.5	REPORTS BY CONTRACTOR	21
3.6	RULES AND REGULATIONS	22
3.7	CONTRACTOR’S STAFF IDENTIFICATION	22
4.	CHANGES NOTICES AND AMENDMENTS	22
4.1	GENERAL	22
4.2	CHANGE NOTICES	23
4.3	AMENDMENTS	23
4.4	PROJECT SCHEDULE	23
4.5	EXTENSIONS OF TIME	23
4.6	BOARD ORDERS	24
4.7	FACSIMILE	24

5.	SCOPE OF WORK.....	24
5.1	SYSTEM COMPONENTS.....	25
5.2	SYSTEM IMPLEMENTATION	25
5.3	SYSTEM MAINTENANCE.....	25
5.4	OPTIONAL WORK.....	25
5.5	STANDARD OF SERVICES.....	26
5.6	UNAPPROVED WORK	26
6.	PROJECT SCHEDULE.....	26
6.1	PROJECT PLAN	26
6.2	KEY DELIVERABLES AND MILESTONES.....	26
7.	TERM	27
7.1	INITIAL TERM.....	27
7.2	EXTENDED TERM	27
7.3	DEFINITION OF TERM	27
7.4	NOTICE OF EXPIRATION	27
8.	CONTRACT SUM	27
8.1	MAXIMUM CONTRACT SUM.....	27
8.2	SYSTEM IMPLEMENTATION	28
8.3	SYSTEM MAINTENANCE.....	28
8.4	OPTIONAL WORK.....	28
8.5	NON-APPROPRIATION OF FUNDS.....	29
8.6	COUNTY'S OBLIGATION FOR FUTURE FISCAL YEARS	29
9.	INVOICES AND PAYMENTS.....	29
9.1	INVOICES	29
9.2	DELIVERY OF SYSTEM SOFTWARE	31
9.3	SALES/USE TAX.....	31

9.4	PAYMENTS	32
9.5	COUNTY'S RIGHT TO WITHHOLD PAYMENT	32
10.	SYSTEM OWNERSHIP AND LICENSE	32
10.1	SYSTEM OWNERSHIP	32
10.2	LICENSE	33
10.3	SOURCE CODE.....	35
11.	SYSTEM ACCEPTANCE.....	37
11.1	SYSTEM TESTS	37
11.2	PRODUCTION USE	37
11.3	OPERATIONAL USE AND FINAL ACCEPTANCE	37
11.4	FAILED TESTING	38
12.	WARRANTIES AND CORRECTION OF DEFICIENCIES	39
12.1	GENERAL WARRANTIES.....	39
12.2	SYSTEM WARRANTIES AND PROBLEM RESOLUTION	39
12.3	CONTINUOUS PRODUCT SUPPORT	40
12.4	WARRANTY PASS-THROUGH	41
12.5	REMEDIES	41
12.6	BREACH OF WARRANTY OBLIGATIONS.....	41
12.7	DISCLAIMER OF WARRANTIES	41
13.	INDEMNIFICATION.....	41
13.1	GENERAL	41
13.2	LIMITATION OF LIABILITY.....	42
14.	INSURANCE.....	42
14.1	GENERAL INSURANCE REQUIREMENTS	42
14.2	EVIDENCE OF COVERAGE AND NOTICE	42
14.3	ADDITIONAL INSURED STATUS AND SCOPE OF COVERAGE	43

14.4	INSURANCE COVERAGE.....	45
14.5	FAILURE TO MAINTAIN COVERAGE.....	46
15.	INTELLECTUAL PROPERTY WARRANTY AND INDEMNIFICATION.....	47
16.	PROPRIETARY CONSIDERATIONS	48
16.1	COUNTY MATERIALS	48
16.2	TRANSFER TO COUNTY	48
16.3	CONTRACTOR’S OBLIGATIONS.....	48
16.4	PROPRIETARY AND CONFIDENTIAL	48
17.	DISCLOSURE OF INFORMATION.....	49
17.1	DISCLOSURE OF AGREEMENT.....	49
17.2	REQUIRED DISCLOSURE	49
18.	CONFIDENTIALITY AND SECURITY	49
18.1	CONFIDENTIALITY	49
18.2	SECURITY.....	50
18.3	REMEDIES	51
19.	ASSIGNMENT AND DELEGATION.....	51
20.	TERMINATION FOR DEFAULT.....	52
21.	TERMINATION FOR CONVENIENCE.....	52
22.	TERMINATION FOR IMPROPER CONSIDERATION.....	53
23.	TERMINATION FOR INSOLVENCY	53
24.	EFFECT OF TERMINATION	54
25.	INDEPENDENT CONTRACTOR STATUS	55
26.	SUBCONTRACTING	55
27.	RISK OF LOSS.....	57
28.	MOST FAVORED PUBLIC ENTITY.....	57
29.	RECORDS AND AUDITS.....	57

30.	COUNTY'S QUALITY ASSURANCE PLAN	58
31.	CONFLICT OF INTEREST	58
32.	COMPLIANCE WITH APPLICABLE LAWS.....	58
33.	FAIR LABOR STANDARDS	59
34.	COMPLIANCE WITH CIVIL RIGHTS LAWS.....	59
35.	RESTRICTIONS ON LOBBYING	61
35.1	FEDERAL FUNDS PROJECTS	61
35.2	LOBBYIST ORDINANCE	61
36.	EMPLOYMENT ELIGIBILITY VERIFICATION	61
37.	CONTRACT HIRING	62
37.1	CONSIDERATION OF HIRING COUNTY EMPLOYEES TARGETED FOR LAYOFFS	62
37.2	CONSIDERATION OF GAIN/GROW PROGRAM PARTICIPANTS FOR EMPLOYMENT	62
37.3	PROHIBITION AGAINST INDUCEMENT AND PERSUASION.....	62
38.	FEDERAL EARNED INCOME CREDIT	62
39.	CONTRACTOR RESPONSIBILITY AND DEBARMENT	62
39.1	RESPONSIBLE CONTRACTOR	62
39.2	CHAPTER 2.202.....	62
39.3	NON-RESPONSIBLE CONTRACTOR	63
39.4	CONTRACTOR HEARING BOARD	63
39.5	SUBCONTRACTORS OF CONTRACTOR	64
40.	FEDERAL ACCESS TO RECORDS.....	64
41.	REQUIRED CERTIFICATIONS.....	64
42.	NO THIRD PARTY BENEFICIARIES	64
43.	CONTRACTOR PERFORMANCE DURING CIVIL UNREST AND DISASTER	65
44.	WARRANTY AGAINST CONTINGENT FEES.....	65

45.	SAFELY SURRENDERED BABY LAW	65
45.1	NOTICE	65
45.2	ACKNOWLEDGMENT OF COMMITMENT	65
46.	COMPLIANCE WITH COUNTY'S JURY SERVICE PROGRAM	65
46.1	JURY SERVICE PROGRAM	65
46.2	WRITTEN EMPLOYEE JURY SERVICE POLICY	66
47.	CONTRACTOR'S WARRANTY OF ADHERENCE TO COUNTY'S CHILD SUPPORT COMPLIANCE PROGRAM	66
48.	TERMINATION FOR BREACH OF WARRANTY TO MAINTAIN COMPLIANCE WITH COUNTY'S CHILD SUPPORT COMPLIANCE PROGRAM.....	67
49.	CHARITABLE ACTIVITIES COMPLIANCE [IF APPLICABLE]	67
50.	DEFAULTED PROPERTY TAX REDUCTION PROGRAM	67
50.1	CONTRACTOR'S WARRANTY OF COMPLIANCE WITH COUNTY'S DEFAULTED PROPERTY TAX REDUCTION PROGRAM.....	67
50.2	TERMINATION FOR BREACH OF WARRANTY TO MAINTAIN COMPLIANCE WITH COUNTY'S DEFAULTED PROPERTY TAX REDUCTION PROGRAM.....	68
51.	COUNTY AUDIT SETTLEMENTS	68
52.	DISPUTE RESOLUTION PROCEDURE	68
53.	ASSIGNMENT BY COUNTY.....	69
54.	NEW TECHNOLOGY	69
55.	NON-DISCRIMINATION IN SERVICES	69
56.	UNLAWFUL SOLICITATION	70
57.	GOVERNING LAW, JURISDICTION AND VENUE	70
58.	WAIVER.....	70
59.	AUTHORIZATION WARRANTY.....	70
60.	VALIDITY AND SEVERABILITY	70
60.1	VALIDITY	70
60.2	SEVERABILITY	71

61.	NOTICES.....	71
62.	ARM'S LENGTH NEGOTIATIONS	71
63.	NON-EXCLUSIVITY	71
64.	CAPTIONS AND PARAGRAPH HEADINGS.....	72
65.	FORCE MAJEURE	72
66.	FORMS AND PROCEDURES	72
67.	DAMAGE TO COUNTY FACILITIES, BUILDINGS AND GROUNDS	72
68.	MINIMUM AGE, LANGUAGE SKILLS AND LEGAL STATUS OF CONTRACTOR PERSONNEL AT FACILITY	72
69.	NOTICE OF DELAYS	72
70.	RE-SOLICITATION OF BIDS AND PROPOSALS	72
71.	NO PAYMENT FOR SERVICES PROVIDED FOLLOWING EXPIRATION OR TERMINATION OF AGREEMENT	73
72.	ACCESS TO COUNTY FACILITIES	73
73.	COUNTY FACILITY OFFICE SPACE	73
74.	PHYSICAL ALTERATIONS	73
75.	STAFF PERFORMANCE WHILE UNDER THE INFLUENCE	74
76.	RECYCLED PAPER	74
77.	TIME OFF FOR VOTING	74
78.	SURVIVAL	74

EXHIBITS

Exhibit A Statement of Work

Attachment A.1 System Requirements

Attachment A.2 Project Deliverables

Attachment A.3 Performance Requirements

Attachment A.4 System Configuration

Attachment A.5 Existing System Report (incorporated by reference)

Exhibit B Pricing Schedule

Schedule B.1 Optional Work Schedule

Schedule B.2 Termination for Convenience Reimbursement

Schedule B.3 Additional Workstations

Exhibit C Project Schedule

Exhibit D Service Level Requirements

Exhibit E Administration of Agreement

Exhibit F Confidentiality and Assignment Agreement

Exhibit G Contractor's EEO Certification

Exhibit H Jury Service Ordinance

Exhibit I Safely Surrendered Baby Law

Exhibit J Source Code Escrow Agreement

Exhibit K Third Party Software License Terms

Exhibit L Request for Proposals (incorporated by reference)

Exhibit M Contractor's Proposal (incorporated by reference)

This Agreement is entered into this ____ day of December, 2014 by and between the County of Los Angeles, a political subdivision of the State of California (hereinafter "County"), and NEC Corporation of America (hereinafter Contractor") (hereinafter collectively also the "parties").

RECITALS

WHEREAS, Contractor is qualified by reason of experience, preparation, equipment, organization, qualifications and staffing to provide to County the Work contemplated by this Agreement; and

WHEREAS, County, by and through its Sheriff's Department, is authorized by, inter alia, California Government Code sections 26227 and 31000 to contract for goods and services, including the work contemplated herein; and

WHEREAS, County issued a Request for Proposals (RFP) for the provision, maintenance and support of Multimodal Biometric Identification System (hereinafter "MBIS") solution (hereinafter "Solution"); and

WHEREAS, Contractor has submitted a proposal to County for the provision and maintenance of the Solution, based on which Contractor has been selected for recommendation for award of this Agreement.

NOW THEREFORE, in consideration of the mutual promises, covenants and conditions set forth herein and for good and valuable consideration, County and Contractor agree as follows:

1. APPLICABLE DOCUMENTS

1.1 INTERPRETATION

The provisions of this document (hereinafter "Base Agreement"), along with Exhibits A, B, C, D, E, F, G, H, I, J and K including all Attachments and Schedules thereto with the exception of Attachment A.5, attached hereto, and Exhibits L and M and Attachment A.5, not attached hereto, all described in this Paragraph 1.1 below and incorporated herein by reference, collectively form and throughout and hereinafter are referred to as the "Agreement". In the event of any conflict or inconsistency in the definition or interpretation of any word, responsibility, schedule or the contents or description of any task, subtask, deliverable, goods, service or other work, or otherwise, between this Base Agreement and the Exhibits, Attachments and Schedules or between the Exhibits, Attachments and Schedules, such conflict or inconsistency shall be resolved by giving precedence first to the Base Agreement, and then to the Exhibits, Attachments and Schedules according to the following descending priority:

Exhibit A – Statement of Work

Attachment A.1 – System Requirements

Attachment A.2 – Project Deliverables

Attachment A.3 – Performance Requirements

Attachment A.4 – System Configuration

Attachment A.5 – Existing System Report (incorporated by reference)

Exhibit B – Pricing Schedule

- Schedule B.1 – Optional Work Schedule
- Schedule B.2 – Termination for Convenience Reimbursement
- Schedule B.3 – Additional Workstations
- Exhibit C – Project Schedule
- Exhibit D – Service Level Requirements
- Exhibit E – Administration of Agreement
- Exhibit F – Confidentiality and Assignment Agreement
- Exhibit G – Contractor's EEO Certification
- Exhibit H – Jury Service Ordinance
- Exhibit I – Safely Surrendered Baby Law
- Exhibit J – Source Code Escrow Agreement
- Exhibit K – Third Party Software License Terms
- Exhibit L – Request for Proposals (incorporated by reference)
- Exhibit M – Contractor's Proposal (incorporated by reference)

1.2 ENTIRE AGREEMENT

This Agreement constitutes the complete and exclusive statement of understanding between the parties and supersedes all previous and contemporaneous agreements, whether written or oral, and any and all communications and negotiations between the parties relating to the subject matter of this Agreement.

1.3 DEFINITIONS

The terms and phrases in this Paragraph 1.3 in quotes and with initial letter capitalized, where applicable, whether singular or plural, shall have the particular meanings set forth below whenever such terms are used in this Agreement.

1.3.1 ACCEPTANCE

The term "Acceptance" shall mean County's written approval of any tasks, subtasks, deliverables, goods, services or other Work, including System Tests, provided by Contractor to County pursuant to this Agreement.

1.3.2 ADDITIONAL CUSTOMIZATIONS

The term "Additional Customization(s)" shall mean configurations and any other customizations of Application Software, and related Documentation, that Contractor may provide following Final Acceptance upon County's request therefor as Programming Modifications in accordance with Paragraph 5.4 (Optional Work), which will update Schedule B.1 (Optional Work Schedule). Once accepted and approved by County, Additional Customizations shall become part of, and be deemed, Application Software for the purpose of this Agreement.

1.3.3 ADDITIONAL HARDWARE

The term "Additional Hardware" shall mean the hardware and other equipment, and related Documentation, that Contractor may provide as part of Optional Work upon County's

request therefor as Additional Products in accordance with Paragraph 5.4 (Optional Work), which will update Schedule B.1 (Optional Work Schedule). Once accepted and approved by County, Additional Hardware shall become part of, and be deemed, System Hardware for the purpose of this Agreement.

1.3.4 ADDITIONAL INTERFACES

The term "Additional Interface(s)" shall mean Interfaces, and related Documentation, that Contractor may provide following Final Acceptance upon County's request therefor as Software Modifications in accordance with Paragraph 5.4 (Optional Work), which will update Schedule B.1 (Optional Work Schedule). Once accepted and approved by County, Additional Interfaces shall become part of, and be deemed, Application Software for the purpose of this Agreement.

1.3.5 ADDITIONAL PRODUCTS

The term "Additional Product(s)" shall mean any item of Additional Software or Additional Hardware, including Additional Workstations, and related Documentation, that Contractor may provide as part of Optional Work upon County's request therefor.

1.3.6 ADDITIONAL SOFTWARE

The term "Additional Software" shall mean additional applications or licenses that are part of Application Software, and related Documentation, that Contractor may provide following Final Acceptance upon County's request therefor in accordance with Paragraph 5.4 (Optional Work), which will update Schedule B.1 (Optional Work Schedule). Once accepted and approved by County, Additional Software shall become part of, and be deemed, Application Software for the purpose of this Agreement.

1.3.7 ADDITIONAL TRAINING

The term "Additional Training" shall mean the Training regarding the Solution, which Contractor may provide following Final Acceptance upon County's request therefor as Professional Services in accordance with Paragraph 5.4 (Optional Work), which will update Schedule B.1 (Optional Work Schedule).

1.3.8 ADDITIONAL WORKSTATION

The term "Additional Workstation" shall mean computer terminals with installed software, capable of interfacing with MBIS, that may be provided by Contractor to County by Change Notice or Amendment, as applicable, as Additional Products using Pool Dollars for performance of Work under the Agreement.

1.3.9 AGREEMENT

The term "Agreement" shall have the meaning specified in Paragraph 1.1 (Interpretation) above.

1.3.10 AMENDMENT

The term "Amendment" shall have the meaning specified in Paragraph 4 (Changes Notices and Amendments).

1.3.11 ANNUAL FEES

The term "Annual Fee(s)" shall mean the annual portion of the Service Fees to be paid by County to Contractor for System Maintenance for Maintenance Periods commencing upon

Final Acceptance in accordance with the terms of this Agreement, including Exhibit B (Pricing Schedule).

1.3.12 APPLICATION MODIFICATIONS

The term "Application Modification(s)" shall mean Programming Modifications including Additional Customizations and Additional Interfaces, and related Documentation, that Contractor may provide following Final Acceptance upon County's request therefor as Optional Work in accordance with Paragraph 5.4 (Optional Work), which will update Schedule B.1 (Optional Work Schedule).

1.3.13 APPLICATION SOFTWARE

The term "Application Software" shall mean all Baseline Application, Interfaces, Third Party Application, Applications Modifications and Customizations, and related Documentation, provided by Contractor to County as part of the Solution in accordance with the terms of this Agreement.

1.3.14 BASE AGREEMENT

The term "Base Agreement" shall have the meaning specified in Paragraph 1.1 (Interpretation) above.

1.3.15 BASELINE APPLICATION

The term "Baseline Application" shall mean Core Application including Core Application, Baseline Customizations and Baseline Interfaces, and related Documentation, provided and implemented by Contractor pursuant to this Agreement as part of the System Implementation Services, which shall meet some or all System Requirements.

1.3.16 BASELINE CUSTOMIZATIONS

The term "Baseline Customization(s)" shall mean the Programming Modifications to the Core Application, and related Documentation, provided by Contractor pursuant to this Agreement as part of the Baseline Application, which shall meet some or all System Requirements.

1.3.17 BASELINE HARDWARE

The term "Baseline Hardware" shall mean the hardware and networking equipment, and related Documentation, provided and installed by Contractor pursuant to this Agreement as part of System Implementation Services, which shall meet some or all System Requirements.

1.3.18 BASELINE INTERFACES

The term "Baseline Interface(s)" shall mean Interfaces, and related Documentation, provided by Contractor pursuant to this Agreement as part of the Baseline Application, which shall meet some or all System Requirements.

1.3.19 BOARD OF SUPERVISORS; BOARD

The terms "Board of Supervisors" and "Board" shall mean County's Board of Supervisors, which is the governing body of County.

1.3.20 BUSINESS DAY

The term "Business Day" shall mean any day of eight (8) working hours from 8:00 a.m. to 5:00 p.m. Pacific Time (PT), Monday through Friday, excluding County observed holidays.

1.3.21 CHANGE NOTICE

The term "Change Notice" shall have the meaning specified in Paragraph 4 (Changes Notices and Amendments).

1.3.22 CONFIDENTIAL INFORMATION

The term "Confidential Information" shall mean any data or information, in any format, and includes sensitive financial information, any County data and any other information otherwise deemed confidential by County or by Contractor or by applicable Federal, State or local law, as further specified in Paragraph 18 (Confidentiality and Security).

1.3.23 CONSULTING SERVICES

The term "Consulting Services" shall mean Professional Services that Contractor may provide following Final Acceptance upon County's request therefor in accordance with Paragraph 5.4 (Optional Work), which will update Schedule B.1 (Optional Work Schedule).

1.3.24 CONTRACT SUM

The term "Contract Sum" shall mean the total monetary amount payable by County to Contractor hereunder, as set forth in Paragraph 8.1 (Maximum Contract Sum). The Contract Sum shall not be adjusted for any costs or expenses whatsoever of Contractor.

1.3.25 CONTRACTOR

The term "Contractor" shall have the meaning specified in the Recitals to the Agreement.

1.3.26 CONTRACTOR KEY PERSONNEL

The term "Contractor Key Personnel" shall have the meaning specified in Paragraph 3.1 (Contractor Administration).

1.3.27 CONTRACTOR KEY STAFF

The term "Contractor Key Staff" shall have the meaning specified in Paragraph 3.3 (Approval of Contractor's Staff).

1.3.28 CONTRACTOR'S PROJECT DIRECTOR

The term "Contractor's Project Director" shall have the meaning specified in Paragraph 3.2.1 (Contractor's Project Director).

1.3.29 CONTRACTOR'S PROJECT EXECUTIVE

The term "Contractor's Project Executive" shall be the person designated as such in Section 2 (Contractor Key Personnel) of Exhibit E (Administration of Agreement).

1.3.30 CONTRACTOR'S PROJECT MANAGER

The term "Contractor's Project Manager" shall have the meaning specified in Paragraph 3.2.2 (Contractor's Project Manager).

1.3.31 COOP PLAN

The term "COOP Plan" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.32 COOP SITE

The term "COOP Site" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.33 CORE APPLICATION

The term "Core Application" shall mean Contractor's pre-developed software and other tools, and related Documentation, provided by Contractor pursuant to this Agreement as part of the Baseline Application, which shall meet some or all System Requirements.

1.3.34 COTS

The term "COTS" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.35 COUNTY

The term "County" shall mean the County of Los Angeles, California, including its Sheriff's Department.

1.3.36 COUNTY KEY PERSONNEL

The term "County Key Personnel" shall have the meaning specified in Paragraph 2.1 (County Administration).

1.3.37 COUNTY MATERIALS

The term "County Materials" shall have the meaning specified in Paragraph 16.1 (County Materials).

1.3.38 COUNTY SOFTWARE

The term "County Software" shall mean any County software installed and utilized by County in the System Environment.

1.3.39 COUNTY'S PROJECT DIRECTOR

The term "County's Project Director" shall have the meaning specified in Paragraph 2.2.1 (County's Project Director).

1.3.40 COUNTY'S PROJECT MANAGER

The term "County's Project Manager" shall have the meaning specified in Paragraph 2.2.2 (County's Project Manager).

1.3.41 CRITICAL DEFICIENCY

The term "Critical Deficiency" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.42 CUSTOMER SUPPORT

The term "Customer Support" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.43 CUSTOMIZATIONS

The term "Customization(s)" shall mean the customizations or other modifications to the Application Software, including Baseline Customizations and Additional Customizations, and related Documentation, which may be provided by Contractor during the term of the

Agreement upon County's election in order for the Solution to meet existing or future System Requirements selected by County.

1.3.44 DATA MIGRATION

The term "Data Migration" shall mean migration of Existing Data as part of System Implementation Services, as further specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.45 DAY

The term "Day" shall mean calendar day and not Business Day.

1.3.46 DEFICIENCY; DEFICIENCIES

The terms "Deficiency" and "Deficiencies", whether singular or plural, shall mean any of the following: any malfunction, error or defect in the design, development, implementation, materials, and/or workmanship; any failure to meet or comply with or deviation from System Requirements, Specifications, County approved deliverables, any published and/or mutually agreed upon standards or any other representations or warranties by Contractor under the Agreement regarding the Solution; and/or any other problem which results in the Solution, or any component thereof, not performing in compliance with the provisions of this Agreement, including but not limited to the Specifications and System Requirements.

1.3.47 DELIVERABLE; DELIVERABLE

The terms "Deliverable" and "deliverable" shall mean items and/or services provided or to be provided by Contractor under this Agreement, including numbered Deliverable(s) in Exhibit A (Statement of Work).

1.3.48 DEPARTMENT

The term "Department" shall mean County's Sheriff's Department.

1.3.49 DIRECTOR; SHERIFF

The term "Director" and "Sheriff" shall mean the Sheriff of the County of Los Angeles.

1.3.50 DISASTER

The term "Disaster" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.51 DISASTER RECOVERY PLAN; DRP

The terms "Disaster Recovery Plan" and "DRP" shall have the same meaning as the term "COOP Plan".

1.3.52 DISASTER RECOVERY SITE

The term "Disaster Recovery Site" shall have the same meaning as "COOP Site".

1.3.53 DISABLING DEVICE

The term "Disabling Device" shall have the meaning specified in Paragraph 12.1 (General Warranties).

1.3.54 DISASTER RECOVERY

The term "Disaster Recovery" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.55 DISPUTE RESOLUTION PROCEDURE

The term "Dispute Resolution Procedure" shall mean and refer to the provisions of Paragraph 52 (Dispute Resolution Procedure) describing the procedure for resolving the disputes arising under or with respect to this Agreement.

1.3.56 DOCUMENTATION

The term "Documentation" shall mean any and all written and electronic materials provided or made available by Contractor under this Agreement, including, but not limited to, documentation relating to software and hardware specifications and functions, training course materials, Specifications including System Requirements, technical manuals, handbooks, flow charts, technical information, reference materials, user manuals, operating manuals, quick reference guides, FAQs, and all other instructions and reference materials relating to the capabilities, operation, installation and use of the Solution and/or applicable components.

1.3.57 DOWNTIME

The term "Downtime" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.58 DUE DATE

The term "Due Date" shall mean the due date for the completion of any Deliverable in the Project Schedule.

1.3.59 EFFECTIVE DATE

The term "Effective Date" shall mean the date of execution of this Agreement by County and the authorized representative(s) of Contractor.

1.3.60 EXISTING DATA

The term "Existing Data" shall mean the data of any of County's existing systems to be migrated and/or converted by Contractor as part of System Implementation Services in accordance with Exhibit A (Statement of Work).

1.3.61 EXISTING SYSTEM

The term "Existing System" shall mean the system utilized by County on the Effective Date, as further specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.62 EXTENDED TERM

As used herein, the term "Extended Term" shall have the meaning specified in Paragraph 7.2 (Extended Term).

1.3.63 FACTORY ACCEPTANCE TEST; FAT

The terms "Factory Acceptance Test" and "FAT" shall mean shall mean the System Test conducted by Contractor under the Statement of Work, as further specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.64 FAR

The term "FAR" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.65 FINAL ACCEPTANCE

The term "Final Acceptance" shall mean County's written approval in accordance with the terms of this Agreement of Deliverable 7.3 (Final Acceptance) of Exhibit A (Statement of Work).

1.3.66 FINAL ACCEPTANCE DATE

The term "Final Acceptance Date" shall mean the date of Final Acceptance.

1.3.67 FINAL ACCEPTANCE TEST

The term "Final Acceptance Test" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.68 FIXED HOURLY RATE

The term "Fixed Hourly Rate" shall mean the hourly rate, specified in Exhibit B (Pricing Schedule), for Professional Services including Consulting Services and Programming Modifications, as applicable, that Contractor may provide following Final Acceptance upon County's request therefor in the form of Optional Work.

1.3.69 HARDWARE UPGRADES

The term "Hardware Upgrade(s)" shall mean and include any additions to and/or replacements to the System Hardware, available or made available subsequent to Final Acceptance, in order to comply with the System Performance Requirements and other Specifications set forth in the Statement of Work and elsewhere in the Agreement.

1.3.70 IMPLEMENTATION PERIOD

The term "Implementation Period" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.71 INITIAL TERM

The term "Initial Term" shall have the meaning specified in Paragraph 7.1 (Initial Term).

1.3.72 INTERFACED SYSTEM

The term "Interfaced System" shall mean any system interfaced with the Solution as part of the System, including where County Software resides.

1.3.73 INTERFACES

The term "Interface(s)" shall mean the set of software mechanisms, consisting of Baseline Interfaces and Additional Interfaces, which may be provided by Contractor under this Agreement, which allow the transfer of electronic data and/or software commands between computer systems, networks, applications or modules, and related Documentation.

1.3.74 KEY DELIVERABLE

The term "Key Deliverable" shall mean a Deliverable marked as such on Exhibit C (Project Schedule).

1.3.75 LACRIS

The term "LACRIS" shall mean the Los Angeles County Regional Identification System of the County's Sheriff.

1.3.76 LAFIS

The term "LAFIS" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.77 LASD; SHERIFF

The terms "LASD" and "Sheriff" shall have the same meaning as "Department".

1.3.78 LICENSE

The term "License" shall have the meaning specified in Paragraph 10.2 (License).

1.3.79 LOW DEFICIENCY

The term "Low Deficiency" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.80 SERVICE FEES

The term "Service Fee(s)" shall mean and include the fees to be paid by County to Contractor for the provision of System Maintenance, including Maintenance Services and Support Services, in accordance with the terms of this Agreement, including the Statement of Work.

1.3.81 MAINTENANCE PERIOD

The term "Maintenance Period" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.82 MAINTENANCE SERVICES

The term "Maintenance Services" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.83 MAJOR DEFICIENCY

The term "Major Deficiency" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.84 MAXIMUM FIXED PRICE

The term "Maximum Fixed Price" shall mean the maximum amount to be paid by County to Contractor for any Optional Work approved by County to be provided by Contractor in accordance Paragraph 5.4 (Optional Work).

1.3.85 MBIS

The term "MBIS" shall mean a Multimodal Biometric Identification System utilized by the Sheriff and the County Law Enforcement community pursuant to the terms of this Agreement, as further defined in Paragraph 1.3.132 (System) and described in the Recitals to this Base Agreement.

1.3.86 MBIS SOLUTION

The term "MBIS Solution" shall have the same meaning as the term "Solution".

1.3.87 MIGRATION PLAN

The term "Data Migration Plan" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.88 MILESTONE

The term "Milestone" shall mean a Deliverable marked as such on the Project Schedule or considered as a milestone by County.

1.3.89 MODERATE DEFICIENCY

The term "Moderate Deficiency" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.90 MONTHLY FEE

The term "Monthly Fee" shall mean 1/12th of the Annual Fee.

1.3.91 OPERATING SOFTWARE

The term "Operating Software" shall mean the software and other products provided by Contractor as part of the System Environment, including operating and database software.

1.3.92 OPERATIONAL ENVIRONMENT

The term "Operational Environment" shall mean the System Environment set up by Contractor for Operational Use of the Solution as part of System Implementation Services pursuant to Exhibit A (Statement of Work).

1.3.93 OPERATIONAL USE

The term "Operational Use" shall mean the actual use of the Solution in the Operational Environment for the performance of County's operations commencing upon Final Acceptance.

1.3.94 OPTIONAL WORK

The term "Optional Work" shall mean Application Modifications, Professional Services and/or Additional Products that may be provided by Contractor to County upon County's request and approval in accordance with 5.4 (Optional Work) and identified appropriately in Schedule B.1 (Optional Work Schedule).

1.3.95 PHASE 1

The term "Phase 1" shall have the same meaning as "System Implementation Phase".

1.3.96 PHASE 2

The term "Phase 2" shall have the same meaning as "System Operation Phase".

1.3.97 POOL DOLLARS

The term "Pool Dollars" shall mean the amount allocated under this Agreement for the provision by Contractor of Optional Work, including Application Modifications, Professional Services and Additional Products, approved by County in accordance with the terms of this Agreement.

1.3.98 PRICING SCHEDULE

The term "Pricing Schedule" shall mean prices for Deliverables, rates and other fees identified as Exhibit B (Pricing Schedule) with all Schedules thereto.

1.3.99 PRIMARY SITE

The term "Primary Site" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.100 PRIORITY LEVEL

The term "Priority Level" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.101 PROFESSIONAL SERVICES

The term "Professional Service(s)" shall mean Consulting Services and/or Additional Training that Contractor may provide following Final Acceptance upon County's request therefor in the form of Optional Work in accordance with Paragraph 5.4 (Optional Work).

1.3.102 PROGRAMMING MODIFICATIONS

The term "Programming Modification(s)" shall mean the customizations and/or other programming modifications to the Application Software, including Customizations and Interfaces, and related Documentation, which may be provided by Contractor during the term of the Agreement upon County's election in order for the Solution to meet existing or future System Requirements selected by County.

1.3.103 PROJECT PLAN

The term "Project Plan" shall mean the detailed plan for System Implementation Services to be provided by Contractor to County, as further specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.104 PROJECT SCHEDULE

The term "Project Schedule" shall mean the agreed upon timeline for System Implementation Tasks, Subtasks and Deliverables specified in Exhibit A (Statement of Work), identified as Exhibit C (Project Schedule).

1.3.105 RELEASE CONDITIONS

The term "Release Condition(s)" shall have the meaning set forth in Paragraph 10.3.3 (Source Code Release Conditions).

1.3.106 REMOTE SITE

The term "Remote Site" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.107 REPLACEMENT PRODUCT

The term "Replacement Product" shall have the meaning set forth in Paragraph 112.3 (Continuous Product Support).

1.3.108 REQUEST FOR PROPOSALS; RFP

The terms "Request for Proposals" and "RFP" shall mean County's Request for Proposals incorporated into this Agreement as Exhibit L (Request for Proposals).

1.3.109 REQUIRED AGREEMENT

The term "Required Agreement" shall mean and refer to Appendix A (Required Agreement) to the RFP.

1.3.110 RESPONSE TIME

The term "Response Time" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.111 SCHEDULED DOWNTIME

The term "Schedule Downtime" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.112 SCOPE OF WORK

The term "Scope of Work" shall mean the scope of Optional Work agreed by the parties to be provided by Contractor as Optional Work.

1.3.113 SECURITY REQUIREMENTS

The term "Security Requirements" shall mean and refer to the System security requirements specified in the RFP and the Statement of Work.

1.3.114 SELF ESCROW

As used herein, the term "Self Escrow" shall have the meaning specified in Paragraph 10.3.1 (Source Code Escrow).

1.3.115 SERVICE AVAILABILITY

The term "Service Availability" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.116 SERVICE CREDITS

The term "Service Credits" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.117 SERVICE LEVEL PLAN

The term "Service Level Plan" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.118 SERVICE LEVELS; SERVICE LEVEL REQUIREMENTS

The terms "Service Level(s)" and "Service Level Requirements" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.119 SERVICES

The term "Services" shall mean System Implementation Services, System Maintenance Services including Maintenance and Support Services, any services that are part of Optional Work and any other services provided by Contractor under this Agreement.

1.3.120 SEVERE DEFICIENCY

The term "Severe Deficiency" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.121 SOFTWARE MODIFICATIONS

The term "Software Modification(s)" shall mean Application Modifications, Software Updates, Additional Software and any Replacement Products, and related Documentation, that may be provided by Contractor to County under this Agreement. Once accepted and approved by County, Software Modifications shall become part of, and be deemed, Application Software for the purpose of this Agreement.

1.3.122 SOFTWARE UPDATES

The term "Software Update(s)" shall mean and include any additions to and/or replacements to the System Software, on an if and when available basis, available or made available subsequent to Final Acceptance, and shall include all Application Software performance and functionality enhancement releases, new Version Releases, System Software upgrades, improvements, interim updates, including fixes and patches, Deficiency corrections, and any other modifications to the Application Software, including but not limited to those required for the Solution to remain in compliance with applicable Federal and State laws and regulations and the terms of this Agreement, provided by Contractor in accordance with the Statement of Work, with all Attachments thereto.

1.3.123 SOLUTION

The term "Solution" shall mean the combination of the software, hardware, hosting services, maintenance, technical support and other Work, including all System Software, System Data, System Environment, Interfaced Systems, Third Party Software, System Implementation Services, System Maintenance Services and other related Services, provided by Contractor to County in accordance with the terms of this Agreement.

1.3.124 SOURCE CODE

The term "Source Code" shall mean the source code for Application Software, to the extent available, developed for or licensed by Contractor to County under this Agreement, including Baseline Application, Application Modifications, Interfaces and Customizations, together with all Documentation and other proprietary information related to such source code.

1.3.125 SOURCE CODE ESCROW

As used herein, the term "Source Code Escrow" shall have the meaning specified in Paragraph 10.3.1 (Source Code Escrow).

1.3.126 SOURCE CODE ESCROW AGREEMENT

As used herein, the term "Source Code Escrow Agreement" shall mean any agreement, including all addenda, amendments and modifications thereto, for depositing into escrow the Source Code for Application Software in accordance with Paragraph 10.3.1 (Source Code Escrow), incorporated into this Agreement by reference as Exhibit J (Source Code Escrow Agreement).

1.3.127 SPECIFICATIONS

The term "Specification(s)" shall mean any or all of the following, as applicable:

- (1) All specifications, requirements and standards set forth in Attachment A.1 (System Requirements) and the Deliverables in Exhibit A (Statement of Work).
- (2) All System Performance Requirements and standards set forth in this Agreement,

including, but not limited to, requirements for Service Availability and Response Time identified in the Statement of Work.

- (3) The Documentation, to the extent not inconsistent with any of the foregoing in this definition.
- (4) All specifications identified as such by Contractor, including, but not limited to, the Project Schedule and the Project Plan, but only to the extent: (i) not inconsistent with any of the foregoing in this Paragraph; and (ii) acceptable to County in its sole discretion.
- (5) All System Environment requirements and certifications provided by Contractor in accordance with this Agreement with respect to the System.
- (6) All requirements and/or specifications added to the Solution by Optional Work, including Application Modifications and Additional Products, and any Solution Updates, including Software Updates and Hardware Upgrades.
- (7) All written and/or electronic materials furnished by or through Contractor regarding the Application Software or the Solution, including functionality, features, capacity, availability, response times, accuracy or any other performance or other System criteria or any element of the System or any System component.

1.3.128 STATE

The term "State" means the State of California.

1.3.129 STATEMENT OF WORK; SOW

The terms "Statement of Work" and "SOW" shall mean the Work to be provided by Contractor pursuant to this Agreement identified in terms of Tasks, Subtasks and Deliverables in Exhibit A (Statement of Work).

1.3.130 SUPPORT HOURS

The term "Support Hours" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.131 SUPPORT SERVICES

The term "Support Services" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.132 SYSTEM

The term "System" shall mean the hardware and software comprising the Solution meeting the requirements of this Agreement and the Statement of Work with all Attachments thereto, including but not limited to the System Software, System Environment and System Data, provided by Contractor in accordance with the terms of this Agreement.

1.3.133 SYSTEM ACCEPTANCE TEST; SAT

The terms "System Acceptance Test" and "SAT" shall mean shall mean the System test conducted by Contractor under the Statement of Work, as further specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.134 SYSTEM DATA

The term "System Data" shall mean the data utilized by the Solution.

1.3.135 SYSTEM ENVIRONMENT

The term "System Environment" shall mean the architectural and operational environment for the Solution provided by Contractor or County, as applicable, as part of the System, and related Documentation, including Operating Software and System Hardware.

1.3.136 SYSTEM HARDWARE

The term "System Hardware" shall mean the hardware and networking equipment, and related Documentation, provided by Contractor as part of the Solution, including Baseline Hardware, Hardware Upgrades and Additional Hardware.

1.3.137 SYSTEM IMPLEMENTATION

The term "System Implementation" shall mean System Environment setup, System and System Software installation, Data Migration, System Tests, System Training and other Work to be provided by Contractor as part of the Solution implementation pursuant to Exhibit A (Statement of Work) up to and including Final Acceptance, as further specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.138 SYSTEM IMPLEMENTATION PHASE

The term "System Implementation Phase" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.139 SYSTEM MAINTENANCE

The term "System Maintenance" shall mean Maintenance Services and Support Services provided by Contractor in accordance with this Agreement, including Section 3 (System Operation) of Exhibit A (Statement of Work), as further specified in Paragraph 5.3 (System Maintenance).

1.3.140 SYSTEM OPERATION

The term "System Operation" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.141 SYSTEM OPERATION PHASE

The term "System Operation Phase" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.142 SYSTEM PERFORMANCE

The term "System Performance" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.143 SYSTEM PERFORMANCE DEFICIENCY

The term "System Performance Deficiency" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.144 SYSTEM PERFORMANCE REQUIREMENTS

The term "System Performance Requirements" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.145 SYSTEM REQUIREMENTS

The term "System Requirements" shall mean business, operational, technical and/or functional requirements relating to the operation or utilization of the System, as specified in Attachment A.1 (System Requirements).

1.3.146 SYSTEM SOFTWARE

The term "System Software" shall mean all Application Software, Third Party Software, Additional Software and any Software Modifications, and related Documentation, provided by Contractor to County as part of the System in accordance with the terms of this Agreement.

1.3.147 SYSTEM TEST

The term "System Test" shall mean shall mean any of the System tests conducted by County or Contractor, as applicable, under the Statement of Work, including, but not limited to, Factory Acceptance Test, System Acceptance Test and User Acceptance Test.

1.3.148 SYSTEM TRAINING

The term "System Training" shall have the meaning as specified in Task 6 (Conduct System Training) of Exhibit A (Statement of Work).

1.3.149 SYSTEM UPDATE(S)

The term "System Update(s)" shall mean and include any additions, replacements or other modifications to the System, including Software Updates and Hardware Upgrades, that may be provided by Contractor in order to meet the requirements of this Agreement, including the Statement of Work with all Attachments thereto and the Specifications.

1.3.150 TASK; TASK; SUBTASK; SUBTASK

The terms "Task", "task", "Subtask" and "subtask" shall mean one of the areas of work to be performed under this Agreement, including those identified as numbered Tasks and Subtasks in Exhibit A (Statement of Work).

1.3.151 THIRD PARTY APPLICATION

The term "Third Party Application" shall mean the portion of the Application Software provided by Contractor to County under this Agreement that is not proprietary to Contractor.

1.3.152 THIRD PARTY SOFTWARE

The term "Third Party Software" shall mean any software of third parties provided by Contractor to County under this Agreement as part of the Solution, including Third Party Application and Operating Software.

1.3.153 TOT

The term "TOT" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.154 TRAINING

The term "Training" shall mean training relating to the Solution to be provided by Contractor pursuant to this Agreement, including initial System Training and Additional Training that County may acquire as part of Professional Services.

1.3.155 TRAINING PLAN

The term "Training Plan" shall have the meaning specified in Subtask 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.156 UNSCHEDULED DOWNTIME

The term "Unscheduled Downtime" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.157 UAT PLAN

The term "UAT Plan" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.158 UNSCHEDULED DOWNTIME

The term "Unscheduled Downtime" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.159 USER

The term "User" shall mean any person authorized by County to access or use the System pursuant to this Agreement.

1.3.160 USER ACCEPTANCE TEST; UAT

The terms "User Acceptance Test" and "UAT" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work) .

1.3.161 VENDOR

The term "Vendor" shall have the meaning specified in Section 1.4 (Definitions) of Exhibit A (Statement of Work).

1.3.162 VERSION RELEASE

The term "Versions Release" shall mean Contractor's Application Software major version upgrade which may contain new software functionalities and features and/or system compatibilities and may be provided by Contractor on an if and when available basis.

1.3.163 WORK

The term "Work" shall mean any and all tasks, subtasks, deliverables, goods, services and other work provided, or to be provided, by or on behalf of Contractor pursuant to this Agreement, including Solution components, System Implementation Services, System Maintenance Services and Optional Work.

1.3.164 WORK PRODUCT

The term "Work Product" shall have the meaning specified in Paragraph 10.1.4 (Work Product).

2. ADMINISTRATION OF AGREEMENT – COUNTY

2.1 COUNTY ADMINISTRATION

All persons administering this Agreement on behalf of County and identified in this Paragraph 2 below (hereinafter "County Key Personnel") are listed in Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement). Unless otherwise specified,

reference to each of the persons listed in such Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement) shall also include his/her designee. County will notify Contractor in writing of any change in the names and/or addresses of County Key Personnel.

No member of County Key Personnel is authorized to make any changes in any of the terms and conditions of this Agreement other than those specifically authorized under Paragraph 4 (Changes Notices and Amendments).

2.2 COUNTY KEY PERSONNEL

2.2.1 COUNTY'S PROJECT DIRECTOR

County's Project Director will be responsible for ensuring that the objectives of this Agreement are met. County's Project Director will have the right at all times to inspect any and all Work provided by or on behalf of Contractor. Unless specified otherwise, County's Project Director shall also include a designee.

2.2.2 COUNTY'S PROJECT MANAGER

County's Project Manager will be responsible for ensuring that the technical, business and operational standards and requirements of this Agreement are met. County's Project Manager will interface with Contractor's Project Manager on a regular basis. County's Project Manager will report to County's Project Director regarding Contractor's performance with respect to business and operational standards and requirements of the Agreement. Unless specified otherwise, County's Project Manager shall be the designee of County's Project Director.

2.3 COUNTY PERSONNEL

All County personnel assigned to this Agreement shall be under the exclusive supervision of County. Contractor understands and agrees that all such County personnel are assigned only for the convenience of County. Contractor hereby represents that its price, Project Schedule, Project Plan and performance hereunder are based solely on the work of Contractor's personnel, except as otherwise expressly provided in this Agreement.

2.4 APPROVAL OF WORK

All Tasks, Subtasks, Deliverables, including Key Deliverables, and other Work provided by Contractor under this Agreement must have County's written approval at a level no lower than County's Project Manager. In no event shall County be liable or responsible for any payment prior to such written approval. Furthermore, County reserves the right to reject any Work not approved by County.

3. ADMINISTRATION OF AGREEMENT – CONTRACTOR

3.1 CONTRACTOR ADMINISTRATION

All persons administering this Agreement on behalf of Contractor and identified in this Paragraph 3 below (hereinafter "Contractor Key Personnel") are listed in Section 2 (Contractor Key Personnel) of Exhibit E (Administration of Agreement). All staff employed by and/or on behalf of Contractor, including the persons listed in such Section 2 (Contractor Key Personnel) of Exhibit E (Administration of Agreement), shall be adults who are fully fluent in both spoken and written English. Contractor shall notify County in writing of any change in the names and/or addresses of Contractor Key Personnel.

3.2 CONTRACTOR KEY PERSONNEL

3.2.1 CONTRACTOR'S PROJECT DIRECTOR

Contractor's Project Director shall be responsible for Contractor's performance of all Work and ensuring Contractor's compliance with this Agreement. Contractor's Project Director shall meet and confer with County's Project Director on a regular basis as required by County and specified in the Statement of Work regarding the overall scope of the project. Such meetings shall be conducted via teleconference or at a time and place agreed to by County's Project Director and Contractor's Project Director.

3.2.2 CONTRACTOR'S PROJECT MANAGER

Contractor's Project Manager shall be responsible for Contractor's day-to-day activities as related to this Agreement and for reporting to County in the manner set forth in Paragraph 3.5 (Reports by Contractor). Contractor's Project Manager shall interface with County's Project Manager on a regular basis to review project progress and discuss project coordination. Such meetings shall be conducted via teleconference or at a time and place agreed to by County's Project Manager and Contractor's Project Manager.

3.3 APPROVAL OF CONTRACTOR'S STAFF

- 3.3.1 In fulfillment of its responsibilities under this Agreement, Contractor shall utilize, and permit utilization of, only staff fully trained and experienced, and as appropriate, licensed or certified in the technology, trades, tasks and subtasks required by this Agreement. Contractor shall supply sufficient staff to discharge its responsibilities hereunder in a timely and efficient manner.
- 3.3.2 County shall have the right to approve or disapprove each member, or proposed member, of Contractor's Project Director, Contractor's Project Manager and any staff providing Services or on-site Work to County under this Agreement or with access to any of County's sensitive information, including County's Confidential Information, (hereinafter "Contractor Key Staff") prior to and during their performance of any Work hereunder, as well as so approving or disapproving any proposed deletions from or other changes in such Contractor Key Staff. County's Project Manager, in his/her reasonable discretion, may require replacement of any member of the Contractor Key Staff performing, or offering to perform, Work hereunder. Contractor shall provide County with a resume of each such proposed initial Contractor Key Staff member and a proposed substitute and an opportunity to interview such person prior to his/her performance of any Work hereunder. Contractor shall have thirty (30) days from the date of County's written request to replace such staff.
- 3.3.3 In addition, Contractor shall provide to County's Project Director an executed Confidentiality and Assignment Agreement (Exhibit F) for each member of the Contractor Key Staff performing Work under this Agreement on or immediately after the Effective Date, but in no event later than the date such member of the Contractor Key Staff first performs Work under this Agreement.
- 3.3.4 Contractor shall, to the maximum extent possible, take all necessary steps to ensure continuity over time of the membership of the group constituting the Contractor Key Staff. Contractor shall promptly fill any Contractor Key Staff vacancy with personnel having qualifications at least equivalent to those of the Contractor Key Staff member(s) being replaced.

3.3.5 In the event Contractor should ever need to remove any member of the Contractor Key Staff from performing Work under this Agreement, Contractor shall provide County with notice at least fifteen (15) days in advance, except in circumstances in which such notice is not possible, and shall work with County on a mutually agreeable transition plan so as to provide an acceptable replacement and ensure project continuity. Should County be dissatisfied with any member of the Contractor Key Staff during the term of the Agreement, Contractor shall replace such person with another to County's satisfaction.

3.3.6 Contractor shall supply sufficient staff to discharge its responsibilities hereunder in a timely and efficient manner.

3.4 BACKGROUND AND SECURITY INVESTIGATIONS

3.4.1 All Contractor staff performing Work under this Agreement shall undergo and pass, to the satisfaction of County, a background investigation as a condition of beginning and continuing Work under this Agreement. Contractor may conduct its own background checks, provided that they comply with County's requirements, as acknowledged by County's Project Manager or designee. County acknowledges that Contractor has provided information detailing Contractor's background check procedures and that the same are acceptable hereunder. If Contractor's procedures for background checks materially change, Contractor shall provide County with revised procedures for County's acceptance and acknowledgment thereof. All fees associated with obtaining the background information shall be borne by Contractor, regardless of whether Contractor's staff passes or fails the background clearance investigation.

3.4.2 County may immediately, in its sole discretion, deny or terminate facility access to any Contractor's staff, including subcontractor staff, who do not pass such background investigation(s) to the satisfaction of County and/or whose background or conduct is incompatible with County's facility access.

3.4.3 Disqualification, if any, of Contractor's staff, including subcontractor staff, pursuant to this Paragraph 3.4 shall not relieve Contractor of its obligation to complete all Work in accordance with the terms and conditions of this Agreement.

3.5 REPORTS BY CONTRACTOR

In addition to any reports required elsewhere pursuant to this Agreement including the Statement of Work, in order to control expenditures and to ensure the reporting of all Work provided by Contractor, Contractor shall provide to County's Project Manager as frequently as requested by County's Project Manager, but in no event more frequently than weekly, written reports which shall include, at a minimum, the following information:

- (1) Period covered by the report;
- (2) Overview of the reporting period;
- (3) Tasks, subtasks, deliverables, goods, services and other Work scheduled for the reporting period which were completed;
- (4) Tasks, subtasks, deliverables, goods, services and other Work scheduled the reporting period which were not completed;
- (5) Tasks, subtasks, deliverables, goods, services and other Work not scheduled for but completed in the reporting period.

- (6) Tasks, subtasks, deliverables, goods, services and other Work scheduled to be completed in the next reporting period;
- (7) Issues resolved and to be resolved;
- (8) Summary of project status as of reporting date; and
- (9) Any other information which County may from time-to-time require.

3.6 RULES AND REGULATIONS

During the time when Contractor's employees, subcontractors or agents are at County facilities, such persons shall be subject to the applicable rules and regulations of County facilities. It is the responsibility of Contractor to acquaint such persons, who are to provide Work, with such rules and regulations. In the event that County determines that an employee, subcontractor or agent of Contractor has violated any applicable rule or regulation, County shall notify Contractor, and Contractor shall undertake such remedial or disciplinary measures as Contractor determines appropriate. If the problem is not thereby corrected, then Contractor shall permanently withdraw its employee, subcontractor or agent from the provision of Work upon receipt of written notice from County that: (i) such employee, subcontractor or agent has violated such rules or regulations; or (ii) such employee's, subcontractor's or agent's actions, while on County premises, indicate that the employee, subcontractor or agent may adversely affect the provision of Work. Upon removal of any employee, subcontractor or agent, Contractor shall immediately replace the employee, subcontractor or agent and continue uninterrupted Work hereunder.

3.7 CONTRACTOR'S STAFF IDENTIFICATION

3.7.1 Contractor, at Contractor's cost, shall provide each member of the staff assigned to this Agreement with a visible photo identification badge in accordance with County's specifications. Identification badge specifications may change at the sole discretion of County, and Contractor will be provided new specifications as required. The format and content of the badge is subject to County's approval prior to Contractor implementing the use of the badge. Contractor's staff, while on duty or when entering a County facility or its grounds, shall prominently display the photo identification badge on the upper part of the body.

3.7.2 Contractor shall notify County within one (1) Business Day when staff is terminated from work under this Agreement. Contractor is responsible to retrieve and immediately destroy the staff's County-specified photo identification badge at the time of removal from Work under this Agreement.

If County requests the removal of Contractor's staff, Contractor shall be responsible to retrieve and immediately destroy Contractor staff's County photo identification badge at the time of removal from work under this Agreement.

4. CHANGES NOTICES AND AMENDMENTS

4.1 GENERAL

No representative of either County or Contractor, including those named in this Agreement, is authorized to make any changes in any of the terms, obligations or conditions of this Agreement, except through the procedures set forth in this Paragraph 4. County reserves the right to change any portion of the Work required under this Agreement and to any other

provisions of this Agreement. All such changes shall be accomplished only as provided in this Paragraph 4.

4.2 CHANGE NOTICES

For any change requested by County which does not affect the scope of Work, term, payments or any term or condition of this Agreement or a change authorized by expenditure of Pool Dollars, a written notice of such change (hereinafter "Change Notice") shall be prepared and executed by County's Project Director.

4.3 AMENDMENTS

Except as otherwise provided in this Agreement, for any change requested by County which affects the scope of Work, term, payments, or any term or condition included in this Agreement, a negotiated written Amendment to this Agreement shall be prepared and executed by each of County's Board of Supervisors and Contractor's authorized representative(s).

Notwithstanding the foregoing, (i) in the event a change in California or other state or local sales/use tax relating law, regulation or rate affects any component of the Work under the Agreement, the Director, or designee, is specifically authorized to amend the Agreement to increase the maximum Contract Sum, to add or revise the applicable sales/use taxes, to authorize Contractor to invoice accordingly for any such applicable sales/use taxes under the Agreement and to modify the Agreement otherwise as is necessary to ensure that the Work is in full compliance with such changes in sales/use tax relating law, regulation or rate, as further provided in Paragraph 9.3 (Sales/Use Tax) below; (ii) in the event that, as a result of a substantial expansion of any law enforcement agency supported by MBIS, an acquisition of Additional Workstations is required to support the expansion, the Director, or designee, is specifically authorized to amend the Agreement to acquire such Additional Workstations as Optional Work using Pool Dollars and to increase the amount of available Pool Dollars and the maximum Contract Sum under the Agreement by the total cost of such Additional Workstations accordingly; (iii) and in the event County's Board of Supervisors or Chief Executive Officer, or designee, requires addition and/or change of certain County standard contract terms or conditions, the Director, or designee, is specifically authorized to execute amendments on behalf of County to add and/or change such terms or conditions.

4.4 PROJECT SCHEDULE

Following Contractor's provision of a Project Plan under the Statement of Work, a Project Schedule will be derived for the Work relating to System Implementation Services and, as necessary, for System Maintenance, as described in the Statement Work, which shall update Exhibit C (Project Schedule). Changes to the Project Schedule shall be made upon mutual agreement, in writing, by County's Project Director and Contractor's Project Director by Change Notice or otherwise, provided that County's Project Director's and Contractor's Project Director's agreement to alter the Project Schedule shall not prejudice either party's right to claim that such alterations constitute an Amendment to this Agreement that shall be governed by the terms of Paragraph 4.3 (Amendments) above.

4.5 EXTENSIONS OF TIME

Notwithstanding any other provision of this Paragraph 4, to the extent that extensions of time for Contractor's performance do not impact either the scope of Work or cost of this Agreement, County's Project Director, in his/her sole discretion, may grant Contractor

extensions of time in writing for the Work listed in Exhibit C (Project Schedule), provided such extensions shall not exceed a total of six (6) months beyond Final Acceptance.

4.6 BOARD ORDERS

Notwithstanding any other provision of this Paragraph 4 or Paragraph 21 (Termination for Convenience), Director shall take all appropriate actions to carry out any orders of County's Board of Supervisors relating to this Agreement, and, for this purpose, Director is authorized: to (i) issue written notice(s) of partial or total termination of this Agreement pursuant to Paragraph 21 (Termination for Convenience) without further action by County's Board of Supervisors and/or (ii) prepare and execute Amendment(s) to this Agreement, which shall reduce the scope of Work and the Contract Sum without further action by County's Board of Supervisors.

4.6.1 Such notices of partial or total termination shall be authorized under the following conditions:

- (1) Notices shall be in compliance with all applicable Federal, State and County laws, rules, regulations and ordinances, guidelines and directives.
- (2) Director shall obtain the approval of County Counsel for any notice.
- (3) Director shall file a copy of all notices with the Executive Office of County's Board of Supervisors and County's Chief Executive Office within thirty (30) days after execution of each notice.

4.6.2 Such Amendments shall be authorized under the following conditions:

- (1) Amendments shall be in compliance with all applicable Federal, State, and County laws, rules, regulations and ordinances, guidelines and directives.
- (2) County's Board of Supervisors has appropriated sufficient funds for purposes of such Amendments and this Agreement.
- (3) Director shall obtain the approval of County Counsel for any Amendment.
- (4) Director shall file a copy of all Amendments with the Executive Office of County's Board of Supervisors and County's Chief Executive Office within thirty (30) days after execution of each Amendment.

4.7 FACSIMILE

Except for the parties' initial signatures to this Agreement or any Amendment, which must be provided in "original" form and not by facsimile, County and Contractor hereby agree to regard facsimile representations of original signatures of authorized officials of each party, when appearing in appropriate places on the Change Notices prepared pursuant to this Paragraph 4 and received via communications facilities, as legally sufficient evidence that such original signatures have been affixed to Change Notices to this Agreement, such that the parties need not follow up facsimile transmissions of such documents by subsequent (non-facsimile) transmissions of "original" versions of such documents.

5. SCOPE OF WORK

In exchange for County's payment to Contractor of the applicable Service Fees arising under the Agreement and invoiced by Contractor, Contractor shall (a) on a timely basis provide, complete, deliver and implement all Work set forth in this Agreement, including Exhibit A

(Statement of Work), including but not limited to components of the System, System Implementation Services, System Maintenance Services and any Optional Work; and (b) grant to County the License to the all System Software provided by Contractor under the Agreement, as specified in Paragraph 10.2 (License). Contractor shall perform all such tasks, subtasks, deliverables, goods, services and other Work in accordance with Exhibit A (Statement of Work) with all Attachments thereto and the Service Level Plan with all Schedules thereto at the applicable rates and prices specified in Exhibit B (Pricing Schedule) with all Schedules thereto.

5.1 SYSTEM COMPONENTS

Contractor shall provide the License to all System Software, including but not limited to Application Software, Third Party Software and Software Modifications, and all System Environment components, including Operating Software, System Hardware and Hardware Upgrades, in order to meet the System Requirements as such may be revised during the term of the Agreement, all in accordance with the provisions of Paragraph 10 (System Ownership and License) and the Agreement.

5.2 SYSTEM IMPLEMENTATION

Contractor shall provide System Implementation Services, including but not limited to System setup, installation, testing, training, Baseline Customizations and/or Baseline Interfaces, and other Services through Final Acceptance of the System, as required for the successful implementation of the Solution, as specified in the Statement of Work and elsewhere in the Agreement.

5.3 SYSTEM MAINTENANCE

Contractor shall provide to County System Maintenance Services relating to the hosting, maintenance and support of the Solution, including but not limited to Maintenance Services and Support Services, as provided in, and in accordance with, this Agreement, including the Statement of Work. System Maintenance obligations shall commence upon Final Acceptance and shall continue through the term of this Agreement.

5.4 OPTIONAL WORK

Upon the written request of County's Project Director or designee following Final Acceptance and mutual agreement, Contractor shall provide to County Optional Work using Pool Dollars, including Software Modifications, Professional Services and/or Additional Workstations or other Additional Products. Software Modifications shall only include those products and services relating to the requirements not reflected on the Effective Date in the Specifications including System Requirements, as determined by County's Project Director or designee.

Upon County's request and Contractor's agreement to provide the Optional Work, Contractor shall provide to County within ten (10) Business Days of such request, or such longer period as agreed to by the parties, a proposed Scope of Work and a quote for a Maximum Fixed Price calculated in accordance with the terms set forth in Exhibit B (Pricing Schedule), including the Fixed Hourly Rate, if applicable. Contractor's quotation shall be valid for at least ninety (90) days from submission. Contractor shall commence the Optional Work following agreement by the parties with respect to such Scope of Work and the Maximum Fixed Price. Upon completion by Contractor, and approval by County in accordance with the terms of this Agreement, of such Optional Work, Schedule B.1 (Optional Work Schedule)

shall be updated accordingly to add such items of Optional Work by Change Notice executed in accordance with Paragraph 4 (Changes Notices and Amendments).

Notwithstanding the foregoing under this Paragraph 5.4, upon County's election, County may request and Contractor provide Additional Workstations as Optional Work using Pool Dollars prior to Final Acceptance.

5.5 STANDARD OF SERVICES

Contractor's services and other Work required by this Agreement shall during the term of the Agreement conform to reasonable commercial standards as they exist in Contractor's profession or field of practice. If Contractor's Services or other Work provided under this Agreement fail to conform to such standards, upon notice from County specifying the failure of performance, Contractor shall, at Contractor's sole expense, provide the applicable remedy as specified in this Agreement, including the Statement of Work. Contractor shall, at its own expense, correct any data in which (and to the extent that) errors have been caused by Contractor or malfunctions of the Solution or by any other tools introduced by Contractor into the System for the purpose of performing services or other Work under this Agreement or otherwise.

5.6 UNAPPROVED WORK

If Contractor provides any tasks, subtasks, deliverables, goods, services or other work to County other than those specified in this Agreement, or if Contractor provides such items requiring County's prior written approval without first having obtained such written approval, the same shall be deemed to be a gratuitous effort on the part of Contractor, and Contractor shall have no claim whatsoever against County therefor.

6. PROJECT SCHEDULE

6.1 PROJECT PLAN

Contractor shall implement the Solution in accordance with the Project Schedule, set forth in Exhibit C (Project Schedule), based upon the Project Plan developed and delivered pursuant to the Statement of Work. The Project Schedule shall, at a minimum, include the following items:

- (1) Deliverable Number;
- (2) Description;
- (3) Due Date;
- (4) Milestone/Key Deliverables Number;
- (5) Associated or Dependent Deliverable; and
- (6) Any other items reasonably required by County under this Agreement.

6.2 KEY DELIVERABLES AND MILESTONES

Exhibit C (Project Schedule) shall specify certain Deliverables as Key Deliverables and/or Milestones, as determined by County. A Key Deliverable or a Milestone shall be deemed completed for purposes of this Paragraph 6.2 on the earliest date that all of the tasks, subtasks, deliverables, goods, services and other Work required for completion of such Key Deliverable or Milestone are completed and delivered to County, provided that all of such Work required for completion of such Key Deliverable or Milestone are thereafter approved

in writing by County pursuant to Paragraph 2.4 (Approval of Work) without prior rejection by County or significant delay in County's approval thereof, which delay is the result of Contractor's failure to deliver such tasks, subtasks, deliverables, goods, services and other Work in accordance with the terms hereof. The determination of whether a Key Deliverable or Milestone has been so completed and so approved, and of the date upon which such Key Deliverable or Milestone was completed, shall be made by County's Project Director as soon as practicable in accordance with Paragraph 2.4 (Approval of Work) after County is informed by Contractor that such Key Deliverable or Milestone has been completed and is given all the necessary information, data and documentation to verify such completion.

7. TERM

7.1 INITIAL TERM

The term of this Agreement shall commence upon the Effective Date and shall expire six (6) years following the Final Acceptance of the Solution, unless sooner terminated or extended, in whole or in part, as provided in this Agreement (hereinafter "Initial Term").

7.2 EXTENDED TERM

At the end of the Initial Term, County may, at its sole option, extend this Agreement for additional four (4) years (hereinafter "Extended Term"), subject to, among others, County's right to terminate earlier for convenience, non-appropriation of funds, default of Contractor, substandard performance of Contractor, non-responsibility of Contractor and any other term or condition of the Agreement providing for early termination of the Agreement by County. County will exercise its extension option by notifying Contractor in writing of its election to extend the Agreement pursuant to this Paragraph 7 no later than thirty (30) days prior to the expiration of the Initial Term.

County maintains databases that track/monitor Contractor performance history. Information entered into such databases may be used for a variety of purposes, including determining whether County will exercise an Agreement term extension option.

7.3 DEFINITION OF TERM

As used throughout this Agreement, the word "term" when referring to the term of the Agreement shall include the Initial Term and the Extended Term, to the extent County exercises its extension option pursuant to Paragraph 7.2 (Extended Term).

7.4 NOTICE OF EXPIRATION

Contractor shall notify County when this Agreement is within six (6) months from the expiration of the term. Upon occurrence of this event, Contractor shall send written notification to County's Project Director at the address set forth in Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement).

8. CONTRACT SUM

8.1 MAXIMUM CONTRACT SUM

The Contract Sum under this Agreement shall be the total monetary amount payable by County to Contractor for supplying all the tasks, subtasks, deliverables, goods, services and other Work required or requested by County under this Agreement. All Work completed by Contractor must be approved in writing by County in accordance with Paragraph 2.4 (Approval of Work). If County does not approve work in writing, no payment shall be due

Contractor for that Work. The Contract Sum, including all applicable taxes, if any, authorized by County hereunder shall not exceed Twenty Four Million Four Hundred Twenty Four Thousand Dollars (\$24,424,000), as further detailed in Exhibit B (Pricing Schedule), unless the Contract Sum is modified pursuant to a duly approved Amendment to this Agreement by County's and Contractor's authorized representative(s) pursuant to Paragraph 4 (Changes Notices and Amendments). The Contract Sum under this Agreement shall cover authorized payments for any and all Work provided by Contractor under the Agreement, including all Service Fees and Pool Dollars allocated for the term of the Agreement.

Contractor shall maintain a system of record keeping that will allow Contractor to determine when it has incurred seventy-five percent (75%) of the Contract Sum, including the Pool Dollars expenditures, authorized for this Agreement. Upon occurrence of this event, Contractor shall provide written notification to County's Project Director at the address set forth in Section 1 (County Key Personnel) in Exhibit E (Administration of Agreement). Notwithstanding the foregoing, Contractor's failure to provide such notification shall not constitute a material breach of this Agreement.

8.2 SYSTEM IMPLEMENTATION

Contractor shall provide (i) the License for all System Software, (ii) System Hardware, and (iii) associated System Implementation Services at no cost to County during the System Implementation Phase of the Agreement. Contractor's cost of System Implementation shall be included in the Service Fees to paid by County to Contractor in accordance with Exhibit B (Pricing Schedule).

8.2.1 TERMINATION

In addition to any other remedies available to County under the Agreement, if any Key Deliverable is not completed within thirty (30) days after the applicable Due Date, and thereafter approved in writing by County pursuant to Paragraph 2.4 (Approval of Work), other than as a result of delays caused by acts or omissions of County as determined by Director in his/her reasonable judgment, and unless County's Project Director and Contractor's Project Director have otherwise agreed in writing prior to such date scheduled for completion, then County may, upon written notice to Contractor, terminate this Agreement for default in accordance with Paragraph 20 (Termination for Default), as determined in the sole discretion of County, subject to the cure provisions set forth in Paragraph 20 (Termination for Default).

8.3 SYSTEM MAINTENANCE

Contractor shall, during the term of this Agreement, provide to County System Maintenance Services, including Maintenance Services and Support Services, in exchange for County's payment of the applicable Service Fees in accordance with and as set forth in Exhibit B (Pricing Schedule), with all Schedules thereto. Service Fees will be paid by County to Contractor for Maintenance Periods commencing upon Final Acceptance and shall not exceed the amounts specified in such Exhibit B (Pricing Schedule).

8.4 OPTIONAL WORK

Upon County's request for Optional Work and mutual agreement, Contractor shall provide to County Optional Work using Pool Dollars in accordance with the agreed upon Maximum Fixed Priced and the Scope of Work, as specified in Paragraph 5.4 (Optional Work). Contractor's rates during the term of the Agreement for Optional Work shall be subject to the

applicable pricing terms set forth in Exhibit B (Pricing Schedule), including Schedule B.3 (Additional Workstations) for acquisition of Additional Workstations. Any Optional Work provided by Contractor shall not cause an increase in the Service Fees under this Agreement. Absent an Amendment in accordance with Paragraph 4 (Changes Notices and Amendments) including Paragraph 4.3 (Amendments), the Pool Dollars are the aggregate amount available during the term of this Agreement for Optional Work requested by County and provided by Contractor.

8.5 NON-APPROPRIATION OF FUNDS

County's obligation may be limited if it is payable only and solely from funds appropriated for the purpose of this Agreement. Notwithstanding any other provision of this Agreement, County shall not be obligated for Contractor's performance hereunder or by any provision of this Agreement during any of County's future fiscal years unless and until County's Board of Supervisors appropriates funds for this Agreement in County's budget for each such future fiscal year. In the event that funds are not appropriated for this Agreement, then County shall, at its sole discretion, either (i) terminate this Agreement as of June 30 of the last fiscal year for which funds were appropriated or (ii) reduce the Work provided hereunder in accordance with the funds appropriated, as mutually agreed to by the parties. County will notify Contractor in writing of any such non-appropriation of funds at its election at the earliest possible date.

8.6 COUNTY'S OBLIGATION FOR FUTURE FISCAL YEARS

In the event that County's Board of Supervisors adopts, in any fiscal year, a County Budget which provides for the reductions in the salaries and benefits paid to the majority of County employees and imposes similar reductions with respect to County contracts, County reserves the right to reduce its payment obligation under this Agreement correspondingly for that fiscal year and any subsequent fiscal year during the term of this Agreement (including any extensions), and the services to be provided by Contractor under this Agreement shall also be reduced correspondingly. County's notice to the Contractor regarding said reduction in payment obligations shall be provided within thirty (30) calendar days of the Board of Supervisors' approval of such actions. Except as set forth in the preceding sentence, Contractor shall continue to provide all of the services set forth in this Agreement.

9. INVOICES AND PAYMENTS

9.1 INVOICES

Contractor shall invoice County in accordance with Exhibit B (Pricing Schedule) (i) for Services Fees monthly in arrears for Maintenance Periods commencing upon Final Acceptance, for provision of System Maintenance Services; and (ii) for the actual price expended by Contractor for Optional Work using Pool Dollars, which shall not exceed the Maximum Fixed Price quoted for such Optional Work, following Contractor's completion and County's written approval of the Optional Work on a per Change Notice basis.

9.1.1 SUBMISSION OF INVOICES

Contractor's invoice shall include the charges owed to Contractor by County under the terms of this Agreement as provided in Exhibit B (Pricing Schedule). All invoices and supporting documents under this Agreement shall be submitted to the person designated in Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement) as County's Project

Manager at the address specified in such Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement).

9.1.2 INVOICE DETAILS

Each invoice submitted by Contractor shall include the information below, as applicable:

- (1) Agreement Name and Number;
- (2) The tasks, subtasks, deliverables, goods, services or other Work for which payment is claimed, including System Maintenance Services and Optional Work;
- (3) The price of such tasks, subtasks, deliverables, goods, services or other Work calculated based on the pricing terms set forth in Exhibit B (Pricing Schedule) or any Change Notice, as applicable.
- (4) If applicable, the date of written approval of the tasks, subtasks, deliverables, goods, services or other Work by County's Project Director or designee;
- (5) Indication of any applicable withhold or holdback amounts for payments claimed or reversals thereof;
- (6) Indication of any applicable credits due County under the terms of this Agreement or reversals thereof;
- (7) If applicable, a copy of any applicable Acceptance certificates signed by County's Project Director and County's Project Manager; and
- (8) Any other information required by County's Project Director or designee.

9.1.3 APPROVAL OF INVOICES

All invoices submitted by Contractor to County for payment shall have County's written approval as provided in this Paragraph 9.1, which approval shall not be unreasonably withheld. In no event shall County be liable or responsible for any payment prior to such written approval.

9.1.4 INVOICE DISCREPANCIES

County's Project Director will review each invoice for any discrepancies and will, within thirty (30) days of receipt thereof, notify Contractor in writing of any discrepancies found upon such review and submit a list of disputed charges. Contractor shall review the disputed charges and send a written explanation detailing the basis for the charges within thirty (30) days of receipt of County's notice of discrepancies and disputed charges. If County's Project Director does not receive a written explanation for the charges within such thirty (30) day period, Contractor shall be deemed to have waived its right to justify the original invoice amount, and County, in its sole discretion, shall determine the amount due, if any, to Contractor and pay such amount in satisfaction of the disputed invoice, subject to the Dispute Resolution Procedure.

All County correspondence relating to invoice discrepancies shall be sent by email, followed by hard copy, directly to County's Project Manager with a copy to County's Project Director at the addresses specified in Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement).

DELIVERY OF SYSTEM SOFTWARE

It is in the intent of the parties that if any System Software or Documentation provided by Contractor under this Agreement, including any product of System Maintenance Services any Optional Work, is delivered to County, such System Software shall be delivered (i) in an electronic format (e.g., via electronic mail or internet download) or (ii) personally by Contractor staff who shall load such System Software and Documentation onto County's hardware but who will retain possession of all originals and copies of such tangible media (e.g., CD-ROM, magnetic tape, printed manuals) used to deliver the System Software and Documentation to County.

Any System Software and Documentation that is provided or delivered by Contractor to County in a tangible format shall be F.O.B. Destination. The Contract Sum shown in Paragraph 8.1 (Maximum Contract Sum) includes all amounts necessary for County to reimburse Contractor for all transportation and related insurance charges, if any, on System Software Components and Documentation procured by County from Contractor pursuant to this Agreement. All transportation and related insurance charges, if any, shall be paid directly by Contractor to the applicable carrier. Contractor shall be solely liable and responsible for, and shall indemnify, defend, and hold harmless County from, any and all such transportation and related insurance charges.

SALES/USE TAX

The Contract Sum shown in Paragraph 8 (Contract Sum) shall be deemed to include all amounts necessary for County to reimburse Contractor for all applicable California and other state and local sales/use taxes on all Solution components provided by Contractor to County pursuant to or otherwise due as a result of this Agreement, including, but not limited to, any product of System Maintenance Services and any Optional Work, to the extent applicable. All California sales/use taxes, if any, shall be invoiced by Contractor to County and paid by County to Contractor, and subsequently paid directly by Contractor to the State or other taxing authority.

If during the term of the Agreement, any component of the Work becomes subject to additional or changed California or other state or local sales/use tax, the Agreement will be amended by delegated authority in accordance with Paragraph 4 (Change Notices and Amendments) to add to the Contract Sum or revise such sales/use taxes and to authorize Contractor to invoice accordingly for any such additional or revised sales/use tax under the Agreement.

Contractor shall be solely liable and responsible for, and shall indemnify, defend, and hold harmless County from, any and all such California and other state and local sales/use taxes. Further, Contractor shall be solely liable and responsible for, and shall indemnify, defend, and hold harmless County from, all applicable California and other state and local sales/use tax on all other items provided by Contractor pursuant to this Agreement and shall pay such tax directly to the State or other taxing authority. In addition, Contractor shall be solely responsible for all taxes based on Contractor's income or gross revenue, or personal property taxes levied or assessed on Contractor's personal property to which County does not hold title.

9.4 **PAYMENTS**

Provided that Contractor is not in default under any provision of this Agreement, County will pay all invoice amounts to Contractor within thirty (30) days of receipt of invoices that have not been disputed in accordance with Paragraph 9.1.4 (Invoice Discrepancies) above. County's failure to pay within the thirty (30) day period, however, shall not be deemed as automatic invoice approval or Acceptance by County of any deliverable for which payment is sought, nor shall it entitle Contractor to impose an interest or other penalty on any late payment.

9.5 **COUNTY'S RIGHT TO WITHHOLD PAYMENT**

Notwithstanding any other provision of this Agreement, and in addition to any rights of County given by law or provided in this Agreement, County may upon written notice to Contractor withhold payment for any deliverable while Contractor, with no fault of County, is in default hereunder or default related to Work, provided that payments shall not be unreasonably withheld and County's approval of deliverables and/or Work shall be in accordance with Paragraph 2.4 (Approval of Work).

10. SYSTEM OWNERSHIP AND LICENSE

10.1 **SYSTEM OWNERSHIP**

10.1.1 **SYSTEM ENVIRONMENT**

Contractor acknowledges that County, or the rightful owner, owns all System Environment components provided by County, Additional Hardware and County Software; while Contractor, or the rightful owner, shall retain ownership of all System Environment components provided by Contractor, as may be specified in Attachment A.4 (System Configuration).

10.1.2 **SYSTEM SOFTWARE**

All System Software provided by Contractor to County pursuant to this Agreement, including Application Software, Third Party Software and Software Modifications, and related Documentation, is and shall remain the property of Contractor or any rightful third party owner, with which all proprietary rights shall reside, and which shall be subject to the terms of the License granted pursuant to Paragraph 10.2 (License) below.

10.1.3 **SYSTEM DATA**

All System Data provided or made accessible by County to Contractor is and shall remain the property of County.

10.1.4 **WORK PRODUCT**

Notwithstanding any other provision of this Agreement to the contrary, all pre-existing practices, procedures, materials, development tools and reusable components, including but not limited to Contractor's or its vendors' library of generic, reusable software code, procedures, manuals and business practices as well as any modification or extension of tem (hereinafter "Work Product") are and will remain the sole property of Contractor or its vendors, as applicable. County will have no interest in or claim to the Work Product except to the extent necessary to exercise its rights under this Agreement in accordance with the rights and restrictions set forth herein. Pre-existing practices, procedures, materials, development tools and reusable components that are part of the Work Product include any

routines, libraries, tools, methodologies, processes or technologies created, adapted or used by Contractor in its business generally, including generic, reusable software code components and related documentation which contain the basic components of Contractor's software architecture and which are used in most software projects delivered by Contractor plus all associated intellectual property rights. In addition, notwithstanding any provision of this Agreement to the contrary, Contractor is free to use any ideas, concepts or know-how developed or acquired by Contractor during the performance under this Agreement, other than County Materials, to the extent obtained and retained by Contractor's personnel as impressions and general learning. Contractor, or the rightful owner, shall remain the sole owner of all System Software that is part of Work Product, including Contractor's Application Software, Third Party Software, Software Modifications and related Documentation, and all derivative works therein. Work Product does not include any County Materials previously owned by County or designed or developed by Contractor for County.

10.2 LICENSE

10.2.1 LICENSE GRANT

Subject to the applicable provisions of this Agreement, including this Paragraph 10.2, the Statement of Work and Paragraph 10.1 (System Ownership), Contractor hereby grants to County a license to use the System Software and Work Product, including any related Documentation (hereinafter "License"), by all Users in accordance with the scope set forth in Paragraph 10.2.3 (Scope of License) and subject to the restrictions set forth in Paragraph 10.2.4 (License Restrictions) during the term specified in Paragraph 10.2.2 (License Term) and any mutually agreed limitation on Third Party Software, as may further be specified in each of the applicable Third Party Software License Terms attached hereto as Exhibit K (Third Party Software License Terms). Notwithstanding the foregoing, (i) upon mutual agreement of the parties, County may obtain its own license for any Third Party Software, the term and scope of which shall be subject to the terms of County's agreement with the provider of such Third Party Software; and (ii) Contractor shall comply with all System Software related requirements under this Agreement.

10.2.2 LICENSE TERM

The License granted under this Agreement shall commence upon the earlier of the delivery of a first System Software component to County or the Effective Date and shall continue in perpetuity and without regard to the end of the term of this Agreement, unless otherwise specified herein.

10.2.3 SCOPE OF LICENSE

The License granted by Contractor under this Agreement provides County with the following rights:

- (1) To use, install, integrate with other software, operate and execute the System Software in the System Environment on an unlimited number of computers, servers, local area networks and wide area networks, including web connections, except as otherwise specified in and subject to the limitation set forth in the Statement of Work, by an unlimited number of Users in the conduct of the business of County as provided in the Agreement;
- (2) To use, modify, copy, translate and compile the Application Software after such time as one of the Release Conditions described in Paragraph 10.3.3 (Source Code Release

Conditions) has occurred which would permit County to use the Source Code as provided in this Paragraph 10.2.3 and Paragraph 10.3 (Source Code) below;

- (3) To use, modify, copy and display the Documentation, provided that Contractor is given the opportunity to segregate any Contractor's Confidential Information, including but not limited to Solution and User manuals, as necessary or appropriate for County to enjoy and exercise fully the rights granted under this Agreement and the License;
- (4) To permit third party access to the System Software, the Documentation, the Source Code, or any part thereof, as necessary or appropriate for County to enjoy and exercise fully the rights granted under this Agreement and the License, including for the provision of System Maintenance Services including Software Updates, Software Modifications, Professional Services and other business use or support of the System Software as contemplated by this Agreement; provided, however, without limiting County's rights under this Paragraph 10.2.4(4), County covenants and agrees that it shall not exercise any of the rights contained in this Paragraph 10.2.4(4) unless and until the occurrence of any one of the Release Conditions; and
- (5) Pursuant to Paragraph 53 (Assignment by County), to reproduce and use a reasonable number of copies of the System Software provided by Contractor: (i) by County and permitted assignees, for archive and backup purposes; and (ii) by County, for use by permitted assignees so long as all copies of the System Software contain the proprietary notices appearing on the copies initially furnished to County by Contractor.

10.2.4 LICENSE RESTRICTIONS

County acknowledges and agrees (i) that the System Software provided by Contractor to County under the Agreement, including related Documentation, is the confidential and copyrighted property of Contractor, or its licensors, and all rights therein not expressly granted to County are reserved to Contractor, or its licensors, as applicable; and (ii) that Contractor, or its licensors, retain all proprietary rights in and to the foregoing.

Subsequently, County's License to the System Software provided by Contractor hereunder is limited by the restrictions set forth in this Paragraph 10.2.4. Accordingly, County will not:

- (1) Reverse engineer, disassemble or decompile the Application Software provided by Contractor;
- (2) Transfer, sublicense, rent, lease, convey or assign (unless resulting from an Agreement assignment under Paragraph 53 (Assignment by County) the System Software provided by Contractor;
- (3) Copy or reproduce the System Software provided by Contractor in any way except as reasonably necessary for backup, archival or business continuity purposes;
- (4) Use the System Software provided by Contractor on a timesharing, service bureau, subscription service or rental basis for any third party; or
- (5) Remove, modify or obscure any copyright, trademark or other proprietary rights notices that appear on, or during the use of, the System Software provided by Contractor.

10.3 SOURCE CODE

10.3.1 SOURCE CODE ESCROW

Upon the Effective Date of the Agreement, but no later than Contractor commences any Work hereunder, Contractor shall, at no cost to County, have deposited in Source Code Escrow the Source Code for all Application Software that is part of the Solution (i) with a nationally recognized source code escrow company or (ii) with County (hereinafter "Self Escrow") pursuant to the instructions from County's Project Manager. Contractor shall ensure that County has access to the Source Code for all Application Software, either via delivery to County's Self Escrow or pursuant to the Source Code Escrow Agreement (hereinafter, collectively or alternatively with "Self Escrow", "Source Code Escrow"), as applicable. A copy of each fully executed Source Code Escrow Agreement shall be incorporated herein by reference as Exhibit J (Source Code Escrow Agreement) to this Agreement. There shall be no charge to County for the acquisition and/or maintenance of the Source Code Escrow Agreement under this Agreement.

Contractor shall deposit in Source Code Escrow the Source Code for all Application Software utilized by Contractor for the Solution under this Agreement, including the Core Application, Interfaces, Third Party Application, Customizations and Software Modifications. Contractor shall update the Source Code by depositing in Source Code Escrow the Source Code for all Software Modifications, including Application Modifications, Additional Software, Software Updates, Replacement Products, if any, and any other modifications or enhancements to the deposited Application Software and any Application Software newly licensed or developed for the purpose of this Agreement, promptly upon availability or as otherwise required by County. Contractor's duty to update the Source Code shall continue through the term of this Agreement.

Contractor's duty to deposit and maintain the Source Code in Source Code Escrow shall continue throughout the term of this Agreement, unless one of the Release Conditions occurs which would permit County to obtain and use the Source Code in accordance with the terms of this Paragraph 10.3. Contractor may, by written notice to County, change the Source Code Escrow Agreement for the Source Code upon County's approval in accordance with Paragraph 2.4 (Approval of Work). Any such change shall be accomplished by a Change Notice in accordance with Paragraph 4 (Changes Notices and Amendments) above and shall not modify Contractor's obligations or County's rights with respect to the Source Code under this Agreement.

County acknowledges and agrees that Contractor's biometric matching algorithms shall not be included in the Source Code Escrow Agreement. However, Contractor will provide the compiled form of matching technology with no inclusion of the Source Code.

10.3.2 NATURAL DEGENERATION

The parties acknowledge that as a result of the passage of time alone, the deposited Source Code may be susceptible to loss of quality ("Natural Degeneration"). For the purpose of reducing the risk of Natural Degeneration, Contractor shall deposit in Source Code Escrow a new copy of all deposited Source Code no less frequently than every six (6) months, provided that modifications or updates have occurred. In the event the Source Code or any part of it is destroyed or corrupted, upon County's request, Contractor shall deposit a replacement copy of the Source Code in Source Code Escrow.

10.3.3 SOURCE CODE RELEASE CONDITIONS

In addition to any conditions for release of Source Code identified in any Source Code Escrow Agreement, Contractor shall cause the release of the Source Code to County, and County shall have the right to immediately begin using the Source Code, as provided in Paragraph 10.3.5 (Possession and Use of Source Code), at no charge to County, upon the occurrence of the following events (hereinafter, collectively with the release conditions identified in any Source Code Escrow Agreement, "Release Condition(s)"):

- (1) The insolvency of Contractor, including as set forth in Paragraph 23 (Termination for Insolvency); or
- (2) Contractor is unwilling or unable to provide all System Maintenance Services in accordance with the terms of this Agreement, including the Statement of Work; or
- (3) Contractor ceasing to maintain or support the current version or the last two (2) prior Version Releases of the Application Software for reasons other than County's failure to pay for, or election not to receive, Contractor's System Maintenance Services, and no other qualified entity assuming the obligation to provide such System Maintenance Services, which may result in County's termination of the Agreement for default in accordance with Paragraph 20 (Termination for Default); or
- (4) Successor ceasing to do business with County with respect to this Agreement.

Upon occurrence of any of the Release Conditions, Contractor shall ensure the release of the Source Code to County. Notwithstanding the foregoing, County alone may initiate the release of the Source Code if it believes in good faith that a Release Condition has occurred, subject to the provisions of any Source Code Escrow Agreement, if applicable, and this Paragraph 10.3.3.

10.3.4 COUNTY'S RIGHT TO VERIFY SOURCE CODE

Regardless of whether one of the Release Conditions occurs, County shall have the right, at County's sole expense, to request that Contractor verify the relevance, completeness, currency, accuracy and functionality of the deposited Source Code by, among other things, compiling the Source Code and performing test runs for comparison with the applicable Application Software. In the event such testing demonstrates that the Source Code does not correspond to the applicable Application Software operated by County and maintained by Contractor, Contractor shall reimburse County for all costs and fees incurred in the testing and immediately deposit the correct Source Code in Source Code Escrow.

10.3.5 POSSESSION AND USE OF SOURCE CODE

Upon the occurrence of a Release Condition, County shall be entitled to obtain the Source Code from the Source Code Escrow pursuant to the terms of any Source Code Escrow Agreement or Paragraph 10.3.3 (Source Code Release Conditions). County shall be entitled to use the Source Code as needed to remedy the event of release and mitigate any damages arising from such event, provided that mitigation of damages shall not include the sale or sublicense of the Source Code. Such use will include, but not be limited to, County's right to perform its own support and maintenance, alter or modify the Source Code and/or obtain the benefits sought under this Agreement, subject to the limitations of Paragraph 10.3.6 (Proprietary Rights) below.

10.3.6 PROPRIETARY RIGHTS

Subject to the provisions of Paragraph 10.3.5 (Possession and Use of Source Code) and County's License to, and Contractor's ownership of, the Application Software as provided in Paragraph 10.1 (System Ownership), Source Code obtained by County under the provisions of this Agreement shall remain subject to every license restriction, proprietary rights protection and other County obligation specified in this Agreement, provided, however, County may make such Source Code available to third parties as needed to assist it in making authorized use of the Solution. County acknowledges that any possession of the Source Code referred to herein is subject to the confidentiality and proprietary provisions of access to any third party. Should use of the Source Code as provided in this Paragraph 10.3.6 involve the use or practice of any patent, copyright, trade secret, trademark or other proprietary information in which Contractor has an interest, Contractor, on behalf of itself and its assignees and successors, agrees not to assert a claim for patent, copyright, trade secret, trademark or other proprietary information infringement against County or any User provided use of Application Software and Source Code is in accordance with this Agreement.

10.3.7 SOURCE CODE ESCROW AGREEMENT AMENDMENT

As between County and Contractor, this Paragraph 10.3 constitutes an amendment to any Source Code Escrow Agreement and incorporates all of the Release Conditions identified in Paragraph 10.3.3 (Source Code Release Conditions) above.

11. SYSTEM ACCEPTANCE

11.1 SYSTEM TESTS

County and/or Contractor, as applicable, shall conduct all System Tests specified in this Paragraph 11.1 and in the Statement of Work. Such System Tests shall include the following:

- (1) Factory Acceptance Test: As set forth in Subtask 4.1 (Conduct Factory Acceptance Test) of Exhibit A (Statement of Work).
- (2) System Acceptance Test: As set forth in Subtask 4.2 (Conduct System Acceptance Test) of Exhibit A (Statement of Work).
- (3) User Acceptance Test: As set forth in Subtask 4.3 (Conduct User Acceptance Test) of Exhibit A (Statement of Work).
- (4) Final Acceptance Test: As set forth in Subtask 7.4 (Conduct Final Acceptance Test) of Exhibit A (Statement of Work).

11.2 PRODUCTION USE

The System shall achieve Go-Live and shall be ready for Production Use when County's Project Director, or his/her designee, approves in writing Deliverable 9.3 (Go-Live) of Exhibit A (Statement of Work). Such approval by County shall not be unreasonably withheld, delayed or conditioned.

11.3 OPERATIONAL USE AND FINAL ACCEPTANCE

The System shall be ready for Operational Use and achieve Final Acceptance when County's Project Director, or his/her designee, approves in writing Deliverable 7.4 (Final Acceptance) of Exhibit A (Statement of Work). Such approval by County shall not be unreasonably withheld, delayed or conditioned. In the event the System fails to successfully achieve Final

Acceptance, Contractor shall provide to County a diagnosis of the Deficiencies and proposed solution(s). County and Contractor shall agree upon all such proposed solutions prior to their implementation.

11.4 FAILED TESTING

- 11.4.1 If County's Project Director makes a good faith determination at any time that the System as a whole, or any component thereof, has not successfully completed a System Test or has not achieved Final Acceptance (collectively referred to for purposes of this Paragraph 11.4 as "Designated Test"), County's Project Director shall promptly notify Contractor in writing of such failure, specifying with as much detail as possible the manner in which the System component or the System failed to pass the applicable Designated Test. Contractor shall immediately commence all reasonable efforts to complete, as quickly as possible, such necessary corrections, repairs and modifications to the System component or the System as will permit the System component or the System to be ready for retesting. Contractor shall notify County's Project Director in writing when such corrections, repairs and modifications have been completed, and the applicable Designated Test shall begin again. If, after the applicable Designated Test has been completed for a second time, County's Project Director makes a good faith determination that the System component or the System again fails to pass the applicable Designated Test, County's Project Director shall promptly notify Contractor in writing, specifying with as much detail as possible the manner in which the System component or the System failed to pass the applicable Designated Test. Contractor shall immediately commence all reasonable efforts to complete, as quickly as possible, such necessary corrections, repairs and modifications to the System component or the System as will permit the System component or the System to be ready for retesting.
- 11.4.2 Such procedure shall continue, Paragraph 8.2.1 (Termination) in the event Contractor fails to timely complete any Key Deliverable until such time as County notifies Contractor in writing either: (i) of the successful completion of such Designated Test or (ii) that County has concluded that satisfactory progress toward such successful completion of such Designated Test is not being made, in which latter event, County shall have the right to make a determination, which shall be binding and conclusive on Contractor, that a non-curable default has occurred and to terminate this Agreement in accordance with Paragraph 20 (Termination for Default) on the basis of such non-curable default. In the event Contractor, using good faith effort, is unable to cure a deficiency by re-performance after two (2) attempts, County and Contractor will work together to agree on a mutually acceptable resolution, provided that if County and Contractor cannot agree on a resolution, County may terminate this Agreement for default pursuant to Paragraph 20 (Termination for Default).
- 11.4.3 Such a termination for default by County shall be either, as determined by County in its sole judgment: (i) a termination with respect to one or more of the components of the System; or (ii) if County believes the failure to pass the applicable Designated Test materially affects the functionality, performance or desirability to County of the System as a whole, the entire Agreement. In the event of a termination under this Paragraph 11.4, County shall have the right to receive from Contractor reimbursement of all payments made to Contractor by County under this Agreement for the System component(s) and related Deliverables as to which the termination applies or if the entire Agreement is terminated, all amounts paid by County to Contractor under this Agreement. If the termination applies only to one or more System component(s), at County's sole option, any reimbursement due to it may be credited against other sums due and payable by County to Contractor. The foregoing is without

prejudice to any other rights that may accrue to County or Contractor under the terms of this Agreement or by law. Accordingly, in the event of such termination, County shall promptly return to Contractor all System component(s) and related Deliverables to which such termination applies, plus any of Contractor's property, including Contractor's Work Product or any proprietary software or hardware owned by Contractor; and all software licensing rights shall immediately be terminated.

12. WARRANTIES AND CORRECTION OF DEFICIENCIES

12.1 GENERAL WARRANTIES

Contractor represents, warrants, covenants and agrees that throughout the term of this Agreement:

1. Contractor shall comply with the description and representations (including, but not limited to, Deliverable documentation, performance capabilities, accuracy, completeness, characteristics, specifications, configurations, standards, functions and requirements applicable to professional software design meeting industry standards) set forth in this Agreement, including the Exhibit A (Statement of Work) including all Attachments thereto and System Requirements.
2. Unless specified otherwise herein, the Solution shall be free from any and all material Deficiencies.
3. The System Maintenance service levels shall not degrade during the term of the Agreement.
4. Contractor shall not intentionally cause any unplanned interruption of the operations of, or accessibility to the System or any component through any device, method or means including, without limitation, the use of any "virus", "lockup", "time bomb", or "key lock", "worm", "back door" or "Trojan Horse" device or program, or any disabling code, which has the potential or capability of compromising the security of County's confidential or proprietary information or of causing any unplanned interruption of the operations of, or accessibility of the System or any component to County or any User or which could alter, destroy, or inhibit the use of the System or any component, or the data contained therein (collectively referred to as "Disabling Device(s)"), which could block access to or prevent the use of the System or any component by County or Users. Contractor represents, warrants, and agrees that it has not purposely placed, nor is it aware of, any Disabling Device in any System component provided to County under this Agreement, nor shall Contractor knowingly permit any subsequently delivered or provided System component to contain any Disabling Device.

In addition, Contractor shall prevent viruses from being incorporated or introduced into the System or updates or enhancements thereto prior to the installation onto the System and shall prevent any viruses from being incorporated or introduced in the process of Contractor's performance of on-line support.

12.2 SYSTEM WARRANTIES AND PROBLEM RESOLUTION

Contractor hereby warrants that all Deficiencies reported or discovered shall be corrected in accordance with the Statement of Work and the Service Level Plan and shall be at no cost to County beyond the payment of the applicable Service Fees.

Contractor also represents, warrants, covenants and agrees that throughout the term of this Agreement:

1. All System components shall interface and be compatible with each other; and the System components, when taken together, shall be capable of delivering all of the functionality as set forth in this Agreement.
2. The System shall be fully compatible with the rest of the Solution components and any enhancements or upgrades shall be backward compatible with the County's standard browser(s) and operating system version(s) operated on County workstations.
3. The Solution, including the System, shall be capable of delivering all of the functionality and meeting all requirements as set forth in this Agreement, including without limitation the System Requirements and the Specifications.
4. The System shall meet the System Performance Requirements within Contractor's control, including but not limited to those relating to Response Time and Service Availability, as further specified in the Statement of Work. All System Performance Deficiencies shall be deemed at a minimum Priority Level 2 for the purpose of the correction of Deficiencies and other County remedies.

12.3 CONTINUOUS PRODUCT SUPPORT

- 12.3.1 In the event that Contractor replaces any or all components of the Application Software with other software modules or components (hereinafter "Replacement Product") during the term of the Agreement in order to fulfill its obligations under the Agreement and to meet the System Requirements, then the License shall be deemed to automatically include such Replacement Product without cost or penalty to County even if such Replacement Product contains greater functionality than the Application Software it replaced. If required by County, Contractor shall provide the necessary training to County personnel to utilize the Replacement Product at no cost to County.
- 12.3.2 In the event any or all components of the Application Software are migrated to the Replacement Product as a result of an acquisition, sale, assignment, transfer or other change in control of Contractor, then any assignee or successor, by taking benefit (including, without limitation, acceptance of any payment under this Agreement), shall be deemed to have ratified this Agreement. All terms and conditions of this Agreement shall continue in full force and effect for the Replacement Product.
- 12.3.3 The following terms and conditions shall apply if County elects to transfer the License to a Replacement Product:
 - (1) Contractor, or its assignee or successor, shall, at no cost to County, implement the Replacement Product in the System Environment, convert and migrate all of the System Data from the Application Software format to the Replacement Product format to ensure Production Use of such Replacement Product;
 - (2) Any prepaid Service Fees for the Solution shall transfer in full force and effect for the balance of the Replacement Product's maintenance and support term (or equivalent service) at no additional cost. If the prepaid amount is greater than the Replacement Product's maintenance and support fees for the same term, the credit balance shall be applied to future Service Fees or returned to County, at County's option;

- (3) Any and all modules offered separately and needed to match the original Application Software's level of functionality shall be supplied by Contractor, or its assignee or successor, without additional cost or penalty, and shall not affect the calculation of any Annual Fees;
- (4) Contractor shall provide to County the necessary Training for purposes of learning the Replacement Product. Such training shall be provided at no cost to County;
- (5) All License terms and conditions, at a minimum, shall remain as granted herein with no additional fees imposed on County; and
- (6) The definition of Application Software shall include the Replacement Product.

12.4 WARRANTY PASS-THROUGH

Contractor shall assign to County to the fullest extent permitted by law or by this Agreement, and shall otherwise ensure that the benefits of any applicable warranty or indemnity offered by any manufacturer of any System component or any other product or service provided hereunder shall fully extend to and be enjoyed by County.

12.5 REMEDIES

County's remedies under the Agreement for the breach of the warranties set forth in this Agreement, including the Statement of Work, shall include the repair or replacement by Contractor, at Contractor's own option and expense, of the non-conforming System components, any other remedies set forth in the Statement of Work including assessment of Service Credits and any other corrective measures specified in such Statement of Work and this Agreement.

12.6 BREACH OF WARRANTY OBLIGATIONS

Failure by Contractor to timely perform its obligations set forth in this Paragraph 12 shall constitute a material breach, upon which, in addition to County's other rights and remedies set forth herein, County may, after written notice to Contractor and provision of a reasonable cure period, terminate this Agreement in accordance with Paragraph 20 (Termination for Default).

12.7 DISCLAIMER OF WARRANTIES

Except for the warranties expressly set forth in this Paragraph 12, Contractor expressly disclaims all other warranties with respect to the Solution, express or implied, including warranties of merchantability and fitness for a particular purpose. Contractor does not warrant that the Solution will meet any County requirements not expressly included in this Agreement or operate in combination with other products not provided by Contractor, be uninterrupted, operate error free or that the errors will be corrected, unless required under the Agreement, including the Statement of Work.

13. INDEMNIFICATION

13.1 GENERAL

Notwithstanding any provision of this Agreement to the contrary, whether expressly or by implication, Contractor shall indemnify, defend and hold harmless County, its Special Districts, elected and appointed officers, employees, agents and volunteers (hereinafter "County Indemnitees") from and against any and all liability, including but not limited to, demands, claims, actions, fees, costs and expenses (including reasonable attorney and expert

witness fees), directly arising from or connected with Contractor's negligent acts and/or omissions in its performance under this Agreement, except for such loss or damages arising from the sole negligence or willful misconduct of County Indemnitees, provided that (1) Contractor is notified promptly in writing of such actions, suits or other proceedings; (2) County gives Contractor the sole right to defend and, upon written notice to County, settle any suit, provided that Contractor (a) does fulfill its obligation to defend and (b) does not agree to a settlement which may adversely impact County; and (3) County fully cooperates in the defense when and as reasonably requested by Contractor.

Any legal defense pursuant to Contractor's indemnification obligations under this Paragraph 13 shall be conducted by Contractor and performed by counsel selected by Contractor. Notwithstanding the preceding sentence, County shall have the right to participate in any such defense at its sole cost and expense.

13.2 LIMITATION OF LIABILITY

Except for Contractor's indemnity obligations, including as set forth in Paragraph 15 (Intellectual Property Warranty and Indemnification), fraudulent, intentional or willful misconduct, bodily injury or property damage, the total cumulative liability of either party to the other for damages under this Agreement shall be limited to (i) Twelve Million Dollars (\$12,000,000) for the Initial Term, and (ii) Six (6) Million Dollars (\$6,000,000) for the Extended Term.

In no event shall either party be liable to the other for any consequential, indirect, incidental, punitive or special damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of business information and the like), loss of data, incorrectly matched images arising out of this Agreement (whether for breach of contract, tort, negligence or other form of action), even if the party incurring such damages has advised the other party of the possibility of such damages.

14. INSURANCE

14.1 GENERAL INSURANCE REQUIREMENTS

Without limiting Contractor's indemnification of County, and in the performance of this Agreement and until all of its obligations pursuant to this Agreement have been met, Contractor shall provide and maintain at its own expense insurance coverage satisfying the requirements specified in this Paragraph 14. These minimum insurance coverage terms, types and limits ("Required Insurance") also are in addition to and separate from any other contractual obligation imposed upon Contractor pursuant to this Agreement. County in no way warrants that the Required Insurance is sufficient to protect Contractor for liabilities which may arise from or relate to this Agreement.

14.2 EVIDENCE OF COVERAGE AND NOTICE

14.2.1 Certificate(s) of insurance coverage (Certificate) satisfactory to County, and a copy of an Additional Insured endorsement confirming County and its Agents (defined below) has been given Insured status under the Contractor's General Liability policy, shall be delivered to County at the address shown below and provided prior to commencing services under this Agreement.

- 14.2.2 Renewal Certificates shall be provided to County not less than ten (10) days after renewal of Contractor's policy. County reserves the right to obtain copies of relevant sections of any required Contractor and/or subcontractor insurance policies at any time.
- 14.2.3 Certificates shall identify all Required Insurance coverage types and limits specified herein, reference this Agreement by name or number, and be signed by an authorized representative of the insurer(s). The Insured party named on the Certificate shall match the name of Contractor identified as the contracting party in this Agreement. Certificates shall provide the full name of each insurer providing coverage, its NAIC (National Association of Insurance Commissioners) identification number, the amounts of any policy deductibles or self-insured retentions exceeding fifty thousand (\$50,000.00) dollars, and list any County required endorsement forms.
- 14.2.4 Neither County's failure to obtain, nor County's receipt of, or failure to object to a non-complying insurance certificate or endorsement, or any other insurance documentation or information provided by the Contractor, its insurance broker(s) and/or insurer(s), shall be construed as a waiver of any of the Required Insurance provisions.

Certificates and copies of any required endorsements shall be sent to County's Project Director at the address specified in Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement).

Contractor also shall promptly report to County any injury or property damage, accident or incident, including any injury to a Contractor employee occurring on County property, and any loss, disappearance, destruction, misuse, or theft of County property, monies or securities entrusted to Contractor. Such report shall be made in writing within twenty-four (24) hours or the next Business Day. Contractor also shall promptly notify County of any third party claim or suit filed against Contractor or any of its subcontractors which arises from or relates to this Agreement, and could result in the filing of a claim or lawsuit against Contractor and/or County.

14.3 ADDITIONAL INSURED STATUS AND SCOPE OF COVERAGE

The County of Los Angeles, its Special Districts, Elected Officials, Officers, Agents, Employees and Volunteers (collectively County and its Agents) shall be provided additional insured status under Contractor's General Liability and Cyber policy with respect to liability arising out of Contractor's ongoing and completed operations performed on behalf of the County. County and its Agents additional insured status shall apply with respect to liability and defense of suits arising out of Contractor's acts or omissions, whether such liability is attributable to Contractor or to County. The full policy limits and scope of protection also shall apply to County and its Agents as an additional insured, even if they exceed the County's minimum Required Insurance specifications herein. Use of an automatic additional insured endorsement form is acceptable providing it satisfies the Required Insurance provisions herein.

14.3.1 CANCELLATION OF OR CHANGES IN INSURANCE

Contractor shall provide County, or Contractor's insurance policies shall contain, a provision that County shall receive written notice of cancellation or any change in Required Insurance, including insurer, limits of coverage, term of coverage or policy period. The written notice shall be provided to County not less than ten (10) days in advance of cancellation for non-payment of premium and thirty (30) days in advance of any other cancellation or policy

change. Failure to provide written notice of cancellation or any change in Required Insurance may constitute a material breach of this Agreement, in the sole discretion of County, upon which County may suspend or terminate this Agreement.

14.3.2 INSURER FINANCIAL RATINGS

Coverage shall be placed with insurers acceptable to County with A.M. Best ratings of not less than A:VII unless otherwise approved by County.

14.3.3 CONTRACTOR'S INSURANCE SHALL BE PRIMARY

Contractor's insurance policies, with respect to any claims related to this Agreement, shall be primary with respect to all sources of coverage available to Contractor. Any County maintained insurance or self-insurance coverage shall be in excess of and not contribute to any Contractor coverage.

14.3.4 WAIVERS OF SUBROGATION

To the fullest extent permitted by law, Contractor hereby waives its rights and its insurer(s)' rights of recovery against County under all the Required Insurance for any loss arising from or relating to this Agreement. Contractor shall require its insurers to execute any waiver of subrogation endorsements which may be necessary to effect such waiver.

14.3.5 SUBCONTRACTOR INSURANCE COVERAGE REQUIREMENTS

Contractor shall include all subcontractors as insureds under Contractor's own policies, or shall provide County with each subcontractor's separate evidence of insurance coverage. Contractor shall be responsible for verifying each subcontractor complies with the Required Insurance provisions herein, and shall require that each subcontractor name the County and Contractor as additional insureds on the subcontractor's General Liability policy. Contractor shall obtain County's prior review and approval of any subcontractor request for modification of the Required Insurance.

14.3.6 DEDUCTIBLES AND SELF-INSURED RETENTIONS (SIRs)

Contractor's policies shall not obligate County to pay any portion of any Contractor deductible or SIR. County retains the right to require Contractor to reduce or eliminate policy deductibles and SIRs as respects County or to provide a bond guaranteeing Contractor's payment of all deductibles and SIRs, including all related claims investigation, administration and defense expenses. Such bond shall be executed by a corporate surety licensed to transact business in the State of California.

14.3.7 CLAIMS MADE COVERAGE

If any part of the Required Insurance is written on a claims made basis, any policy retroactive date shall precede the effective date of this Agreement. Contractor understands and agrees it shall maintain such coverage for a period of not less than three (3) years following Agreement expiration, termination or cancellation.

14.3.8 APPLICATION OF EXCESS LIABILITY COVERAGE

Contractor may use a combination of primary, and excess insurance policies which provide coverage as broad as ("follow form" over) the underlying primary policies, to satisfy the Required Insurance provisions.

14.3.9 SEPARATION OF INSURED

All liability policies shall provide cross-liability coverage as would be afforded by the standard ISO (Insurance Services Office, Inc.) separation of insureds provision with no insured versus insured exclusions or limitations

14.3.10 ALTERNATIVE RISK FINANCING PROGRAMS

County reserves the right to review, and then approve, Contractor use of self-insurance, risk retention groups, risk purchasing groups, pooling arrangements and captive insurance to satisfy the Required Insurance provisions. County and its Agents shall be designated as an Additional covered Party under any approved program.

14.3.11 COUNTY REVIEW AND APPROVAL OF INSURANCE REQUIREMENTS

County reserves the right to review and adjust the required Insurance provisions, conditioned upon County's determination of changes in risk exposures.

14.4 INSURANCE COVERAGE

14.4.1 COMMERCIAL GENERAL LIABILITY INSURANCE

14.4.2 Providing scope of coverage equivalent to ISO policy form CG 00 01, naming County and its Agents as an additional insured, with limits of not less than:

General Aggregate	\$2 million
Products/Completed Operations Aggregate	\$1 million
Personal and Advertising Injury	\$1 million
Each Occurrence	\$1 million

14.4.3 AUTOMOBILE LIABILITY INSURANCE

Providing scope of coverage equivalent to ISO policy form CA 00 01 with limits of not less than \$1 million for bodily injury and property damage, in combined or equivalent split limits, for each single accident. Insurance shall cover liability arising out of Contractor's use of autos pursuant to this Agreement, including owned, leased, hired, and/or non-owned autos, as each may be applicable.

14.4.4 WORKERS' COMPENSATION AND EMPLOYERS' INSURANCE

Insurance or qualified self-insurance satisfying statutory requirements, which includes Employers' Liability coverage with limits of not less than \$1 million per accident. If Contractor will provide leased employees, or, is an employee leasing or temporary staffing firm or a professional employer organization (PEO), coverage also shall include an Alternate Employer Endorsement (providing scope of coverage equivalent to ISO policy form WC 00 03 01 A) naming County as the Alternate Employer, and the endorsement form shall be modified to provide that County will receive not less than thirty (30) days advance written notice of cancellation of this coverage provision. If applicable to Contractor's operations, coverage also shall be arranged to satisfy the requirements of any federal workers or workmen's compensation law or any federal occupational disease law.

14.4.5 PROFESSIONAL LIABILITY/ERRORS AND OMISSIONS

Insurance covering Contractor's liability arising from or related to this Agreement, with limits of not less than \$1 million per claim and \$2 million aggregate. Further, Contractor understands and agrees it shall maintain such coverage for a period of not less than three (3) years following this Agreement's expiration, termination or cancellation.

14.4.6 PROPERTY COVERAGE

If Contractor's given exclusive use of County owned or leased property shall carry property, Contractor coverage at least as broad as that provided by the ISO special causes of loss (ISO policy form CP 10 30) form. County and its Agents shall be named as an Additional Insured and Loss Payee on Contractor's insurance as its interests may appear. Automobiles and mobile equipment shall be insured for their actual cash value. Real property and all other personal property shall be insured for their full replacement value.

14.4.7 TECHNOLOGY ERRORS AND OMISSIONS INSURANCE

Insurance, including cover for liabilities arising from errors, omissions, or negligent acts in rendering or failing to render computer or information technology services and technology products. Coverage for violation of software copyright is included. Technology services at a minimum include (1) systems analysis, (2) systems programming, (3) data processing, (4) systems integration, (5) outsourcing including outsourcing development and design, (6) systems design, consulting, development and modification, (7) training services relating to computer software or hardware, (8) management, repair and maintenance of computer products, networks and systems, (9) marketing, selling, servicing, distributing, installing and maintaining computer hardware or software, (10) data entry, modification, verification, maintenance, storage, retrieval or preparation of data output, and any other services provided by Contractor, with limits of \$5 million.

14.4.8 PRIVACY/NETWORK SECURITY (CYBER) INSURANCE

Privacy/Network Security ("Cyber") liability coverage providing protection against liability for (1) privacy breaches (liability directly arising from the loss or disclosure of confidential information, provided that such loss or disclosure is a result of Contractor's negligent acts or willful misconduct), (2) system breach, (3) denial or loss of service, (4) introduction, implantation or spread of malicious software code, (5) unauthorized access to or use of computer systems, with limits of \$5 million. No exclusions/restrictions for unencrypted portable devices/media may be on the policy. The County of Los Angeles, its Special Districts, Elected Officials, Officers, Agents, Employees and Volunteers (collectively County and its Agents) shall be provided additional insured status.

14.5 FAILURE TO MAINTAIN COVERAGE

Contractor's failure to maintain or to provide acceptable evidence that it maintains the Required Insurance shall constitute a material breach of the Agreement, upon which County immediately may withhold payments due to Contractor and/or suspend or terminate this Agreement. County, at its sole discretion, may obtain damages from Contractor resulting from such breach. Alternatively, County may purchase the required insurance coverage and, without further notice to Contractor, deduct from sums due to Contractor any premium costs advanced by County for such insurance.

15. INTELLECTUAL PROPERTY WARRANTY AND INDEMNIFICATION

- 15.1 Contractor represents and warrants: (i) that Contractor has the full power and authority to grant the License, ownership and all other rights granted by this Agreement to County; (ii) that no consent of any other person or entity is required by Contractor to grant such rights other than consents that have been obtained and are in effect; (iii) that County is entitled to use the System without interruption, subject only to County's obligation to make the required payments and observe the License terms under this Agreement; (iv) that this Agreement and the System licensed or acquired herein, are neither subject to any liens, encumbrances, or pledges nor subordinate to any right or claim of any third party, including Contractor's creditors; (v) that during the term of this Agreement, Contractor shall not subordinate this Agreement or any of its rights hereunder to any third party without the prior written consent of County, and without providing in such subordination instrument for non-disturbance of County's use of the System (or any part thereof) in accordance with this Agreement; and (vi) that neither the performance of this Agreement by Contractor, nor the License to or ownership by, and use by, County and its Users of the System in accordance with this Agreement will in any way violate any non-disclosure agreement relating to this Agreement, nor constitute any infringement or other violation of, any U.S. copyright, trade secret, trademark, service mark, patent, invention, proprietary information, or other rights of any third party.
- 15.2 Notwithstanding any provision to the contrary, whether expressly or by implication, Contractor shall indemnify, defend, and hold harmless the County its Special Districts, elected and appointed officers, employees and agents (collectively referred to for purposes of this Paragraph 13 as "County") from and against any and all liability, including but not limited to demands, claims, actions, fees, damages, costs, and expenses (including attorneys and expert witness fees) arising from any alleged or actual infringement of any third party's U.S. patent or copyright, or any alleged or actual unauthorized trade secret disclosure, arising from or related to this Agreement and/or the operation and use of the System (collectively referred to for purposes of this Paragraph 13 as "Infringement Claim(s)"). Any legal defense pursuant to Contractor's indemnification obligations under this Paragraph 15.2 shall be conducted by Contractor and performed by counsel selected by Contractor. County shall provide Contractor with information, reasonable assistance, and authority to defend or settle the claim. Notwithstanding the foregoing, County shall have the right to participate in any such defense at its sole cost and expense.
- 15.3 County shall notify Contractor, in writing, as soon as practicable of any claim or action alleging such infringement or unauthorized disclosure. Upon such notice by County, Contractor shall, at its election, at no cost to County, as remedial measures, either: (i) procure the right, by license or otherwise, for County to continue to use the Solution or affected component(s) thereof, or part(s) thereof, to the same extent of County's License or ownership rights under this Agreement; or (ii) to the extent procuring such right to use the Solution is not commercially reasonable, replace or modify the System or component(s) thereof with another software or component(s) thereof of at least equivalent quality and performance capabilities, as mutually determined by County and Contractor until the Solution and all components thereof become non-infringing, non-misappropriating and non-disclosing (hereinafter collectively for the purpose of this Paragraph 15.3 "Remedial Act(s)").
- 15.4 If Contractor fails to complete the Remedial Acts described in Paragraph 15.3 above, then County may terminate this Agreement for default pursuant to Paragraph 20 (Termination for

Default). Notwithstanding any provision to the contrary, refund amounts, if any, shall be calculated based upon the terms of the applicable termination provisions.

16. PROPRIETARY CONSIDERATIONS

16.1 COUNTY MATERIALS

Contractor and County agree that all materials, plans, reports, Project Schedule, Project Plan, documentation and training materials developed by or solely for County, departmental procedures and processes, algorithms and any other information provided by County or specifically provided by Contractor for County pursuant to this Agreement, excluding the Work Product and System Software provided by Contractor and related Documentation (collectively "County Materials"), and all copyrights, patent rights, trade secret rights and other proprietary rights therein shall be the sole property of County. Contractor hereby assigns and transfers to County all of Contractor's right, title, and interest in and to all such County Materials, provided that notwithstanding such County ownership, Contractor may retain possession of all working papers prepared by Contractor. During and for a minimum of five (5) years subsequent to the term of this Agreement, Contractor shall retain any and all such working papers. County shall have the right to inspect any and all such working papers, make copies thereof, and use the working papers and the information contained therein.

16.2 TRANSFER TO COUNTY

Upon request of County, Contractor shall execute all documents reasonably requested by County and shall perform all other reasonable acts requested by County to assign and transfer to, and vest in, County all Contractor's right, title and interest in and to the County Materials, including, but not limited to, all copyright, patent and trade secret rights. County shall have the right to register all copyrights and patents in the name of County of Los Angeles. All material expense of effecting such assignment and transfer of rights shall be borne by County. Further, County shall have the right to assign, license or otherwise transfer any and all County's right, title and interest, including, but not limited to, copyrights and patents, in and to the County Materials.

16.3 CONTRACTOR'S OBLIGATIONS

Contractor shall protect the security of and keep confidential all County Materials and shall use whatever security measures are reasonably necessary to protect all such County Materials from loss or damage by any cause, including fire and theft.

16.4 PROPRIETARY AND CONFIDENTIAL

Any and all County Materials which are developed or were originally acquired by Contractor outside the scope of this Agreement, which Contractor desires to use hereunder, and which Contractor considers to be proprietary or confidential, must be specifically identified by Contractor to County's Project Director as proprietary or confidential, and shall be plainly and prominently marked by Contractor as "PROPRIETARY" or "CONFIDENTIAL", if applicable.

Notwithstanding any other provision of this Agreement, County shall not be obligated in any way under this Agreement for:

- (1) Any disclosure of any materials which County is required to make under the California Public Records Act or otherwise by law; or
- (2) Any Contractor's proprietary and/or confidential materials not plainly and prominently

marked with restrictive legends.

17. DISCLOSURE OF INFORMATION

17.1 DISCLOSURE OF AGREEMENT

Contractor shall not disclose any terms or conditions of, or any circumstances or events that occur during the performance of, this Agreement to any person or entity except as may be otherwise provided herein or required by law. In the event Contractor receives any court or administrative agency order, service of process, or request by any person or entity (other than Contractor's professionals) for disclosure of any such details, Contractor shall, to the extent allowed by law or such order, promptly notify County's Project Director. Thereafter, Contractor shall comply with such order, process or request only to the extent required by applicable law. Notwithstanding the preceding sentence, to the extent permitted by law, Contractor shall delay such compliance and cooperate with County to obtain relief from such obligations to disclose until County shall have been given a reasonable opportunity to obtain such relief.

However, in recognizing Contractor's need to identify its services and related clients to sustain itself, County shall not inhibit Contractor from publicizing its role under this Agreement under the following conditions:

- (1) Contractor shall develop all publicity material in a professional manner.
- (2) During the term of this Agreement, Contractor shall not, and shall not authorize another to, publish or disseminate any commercial advertisements, press releases, feature articles, or other materials using the name of County without the prior written consent of County's Project Director for each such item.

Contractor may, without the prior written consent of County, indicate in its proposals and sales materials that it has been awarded this Agreement with the County of Los Angeles, provided that the requirements of this Paragraph 17 shall apply.

17.2 REQUIRED DISCLOSURE

Notwithstanding any other provision of this Agreement, either party may disclose information about the other that: (i) is lawfully in the public domain at the time of disclosure; (ii) is disclosed with the prior written approval of the party to which such information pertains; or (iii) is required by law to be disclosed.

18. CONFIDENTIALITY AND SECURITY

18.1 CONFIDENTIALITY

18.1.1 CONFIDENTIAL INFORMATION

Each party shall protect, secure and keep confidential all records, materials, documents, data and/or other information, including, but not limited to, billing and sensitive financial information, County records, data and information, County Materials, System Data, Work Product, Application Software, health information and any other data, records and information, received, obtained and/or produced under the provisions of this Agreement (hereinafter "Confidential Information"), in accordance with the terms of this Agreement and all applicable Federal, State or local laws, regulations, ordinances, and publicly known guidelines and directives relating to confidentiality. As used in this Agreement, the term "Confidential Information" shall also include records, materials, data and information

deemed confidential by either Party or the applicable law under Paragraph 3.6 (Rules and Regulations). Each party shall use whatever appropriate security measures are necessary to protect such Confidential Information from loss, damage and/or unauthorized dissemination by any cause, including but not limited to fire and theft.

Contractor shall inform all of its officers, employees, agents and subcontractors providing Work hereunder of the confidentiality provisions of this Agreement. Contractor shall ensure that all of its officers, employees, agents and subcontractors performing Work hereunder have entered into confidentiality agreements no less protective of County than the terms of this Agreement, including this Paragraph 18 and Exhibit F (Confidentiality and Assignment Agreement).

18.1.2 DISCLOSURE

With respect to any of County's Confidential Information or any other records, materials, data or information that is obtained by Contractor (hereinafter collectively for the purpose of this Paragraph 18.1.2 "information"), Contractor shall: (i) not use any such information for any purpose whatsoever other than carrying out the express terms of this Agreement; (ii) promptly transmit to County all requests for disclosure of any such information; (iii) not disclose, except as otherwise specifically permitted by this Agreement, any such information to any person or organization other than County without County's prior written authorization that the information is releasable; and (iv) at the expiration or termination of this Agreement, return all such information to County or maintain such information according to the written procedures provided to Contractor by County for this purpose.

Under State law, including Welfare & Institutions Code, Section 10850 and California Department of Social Services (CDSS), Manual of Policies and Procedures, Division 19, Section 10859 et seq. and 17006, all of the case records and information pertaining to individuals receiving aid are confidential and no information related to any individual case or cases shall be in any way relayed to anyone except those employees of County so designated without written authorization from County.

18.1.3 INDEMNIFICATION

Notwithstanding any provision of this Agreement to the contrary, whether expressly or by implication, Contractor shall indemnify, defend and hold harmless County, its officers, employees, and agents, from and against any and all loss, damage, liability and expense, including, but not limited to, defense costs and reasonable legal, accounting and other expert, consulting or professional fees, arising from any disclosure of such records and information by Contractor, its officers, employees, or agents, except for any disclosure authorized by this Paragraph 18.

18.2 SECURITY

18.2.1 SYSTEM SECURITY

Notwithstanding anything to the contrary herein, Contractor shall provide all Work utilizing security technologies and techniques in accordance with the industry standards, Contractor's best practices and applicable County security policies, procedures and requirements provided by County to Contractor in writing as part of the RFP, this Agreement or otherwise as required by law, including those relating to the prevention and detection of fraud or other inappropriate use or access of systems and networks. Without limiting the generality of the foregoing, Contractor shall implement and use network management and maintenance

applications and tools and fraud prevention and detection and encryption technologies and prevent the introduction of any Disabling Device into the System. In no event shall Contractor's actions or inaction result in any situation that is less secure than the security that Contractor then provides for its own systems and data.

18.2.2 SYSTEM DATA SECURITY

Contractor hereby acknowledges the right of privacy of all persons as to whom there exists any System Data or any other County data. Contractor shall protect, secure and keep confidential all System Data in compliance with all federal, state and local laws, rules, regulations, ordinances, and publicly known guidelines and directives, relating to confidentiality and information security, including any breach of the security of the System, such as any unauthorized acquisition of System Data that compromises the security, confidentiality or integrity of personal information. Further, Contractor shall take all reasonable actions necessary or advisable to protect all System Data in its possession, custody or control from loss or damage by any cause, including fire, theft or other catastrophe. In addition, if requested by County's Project Director, Contractor shall provide notification to all persons whose unencrypted personal information was, or is reasonably believed to have been, acquired by any unauthorized person, and the content, method and timing of such notification shall be subject to the prior approval of County's Project Director. Contractor shall not use System Data for any purpose or reason other than to fulfill its obligations under this Agreement.

18.3 REMEDIES

Contractor acknowledges that a breach by Contractor of this Paragraph 18 may result in irreparable injury to County that may not be adequately compensated by monetary damages and that, in addition to County's other rights under this Paragraph 18 and at law and in equity, County shall have the right to seek injunctive relief to enforce the provisions of this Paragraph 18. The provisions of this Paragraph 18 shall survive the expiration or termination of this Agreement.

Contractor shall take all reasonable actions necessary or advisable to protect the System from loss or damage by any cause. Contractor shall bear the full risk of loss or damage to the System and any System Data arising out of any negligent acts or omissions of Contractor. Contractor shall not be responsible for any loss resulting from force majeure or County's sole fault.

19. ASSIGNMENT AND DELEGATION

19.1 Contractor shall not assign its rights and/or delegate its duties under this Agreement, whether in whole or in part, without the prior written consent of County, and any attempted assignment and/or delegation without such consent shall be null and void. County may exercise or withhold consent in its sole discretion. No assignment and/or delegation shall be effective unless and until there is a duly-executed, written amendment to this Agreement. Any payments by County to any approved delegate or assignee on any claim under this Agreement shall be deductible, at County's sole discretion, against the claims, which the Contractor may have against County.

19.2 Shareholders, partners, members, or other equity holders of Contractor may transfer, sell, exchange, assign, or divest themselves of any interest they may have therein. However, in the event any such sale, transfer, exchange, assignment, or divestment is effected in such a

way as to give majority control of Contractor to any person(s), corporation, partnership, or legal entity other than the majority controlling interest therein at the time of execution of the Agreement, such disposition is an assignment requiring the prior consent of County in accordance with the applicable provisions of this Agreement.

- 19.3 Any assumption, assignment, delegation, or takeover of any of Contractor's duties, responsibilities, obligations, or performance of same by any entity other than Contractor, whether through assignment, subcontract, delegation, merger, buyout, or any other mechanism, with or without consideration for any reason whatsoever without County's express written approval shall be a material breach of the Agreement which may result in the termination of this Agreement. In the event of such termination, County shall be entitled to pursue the same remedies against Contractor as it could pursue in the event of default by Contractor.

20. TERMINATION FOR DEFAULT

- 20.1 County may, by written notice to Contractor, terminate the whole or any part of this Agreement if:

- (1) Contractor fails to comply with the requirements set forth in this Agreement, including the Statement of Work; or
- (2) Contractor fails to demonstrate a high probability of timely fulfillment of the performance requirements under this Agreement; or
- (3) Contractor fails to make progress as to endanger performance of this Agreement in accordance with its terms; or
- (4) Contractor in performance of Work under the Agreement fails to comply with the requirements of this Agreement, including but not limited to the Statement of Work and the Service Level Plan; or
- (5) Contractor fails to perform or comply with any other provisions of this Agreement or materially breaches this Agreement; and, unless a shorter cure period is expressly provided in this Agreement, does not cure such failure or fails to correct such failure or breach within thirty (30) days (or such longer period as County may authorize in writing) of receipt of written notice from County specifying such failure or breach, except that Contractor shall not be entitled to any cure period, and County may terminate immediately, in the event that Contractor's failure to perform or comply is not reasonably capable of being cured.

- 20.2 If, after County has given notice of termination under the provisions of this Paragraph 20, it is determined by County that Contractor was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the notice of termination had been issued pursuant to Paragraph 21 (Termination for Convenience).

- 20.3 The rights and remedies of County provided in this Paragraph 20 shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Agreement.

21. TERMINATION FOR CONVENIENCE

- 21.1 This Agreement may be terminated, in whole or in part, permanently or from time to time, when such action is deemed by County to be in its best interest. Termination of Work hereunder shall be effected by notice of termination to Contractor specifying the extent to which performance of work is terminated and the date upon which such termination becomes

effective, which shall be no less than thirty (30) calendar days after the notice is sent. In the event County has purported to terminate this Agreement for default by notice pursuant to Paragraph 20 (Termination for Default) and it has later been determined that Contractor was not in default, no additional notice shall be required upon such determination.

- 21.2 After receipt of a notice of termination, Contractor shall submit to County, in the form and with any certifications as may be prescribed by County, Contractor's termination claim and invoice. Such claim and invoice shall be submitted promptly in accordance with Paragraph 24 (Effect of Termination).
- 21.3 In the event County terminates the Agreement for convenience pursuant to this Paragraph 21 during the Initial Term, County will reimburse Contractor a pro-rata portion of Contractor's initial investment, depending on the effective date of such termination, not to exceed the amounts and in accordance with the terms set forth in Schedule B.2 (Termination for Convenience Reimbursement).

22. TERMINATION FOR IMPROPER CONSIDERATION

- 22.1 County may, by written notice to Contractor, immediately terminate the right of Contractor to proceed under this Agreement if it is found that consideration, in any form, was offered or given by Contractor, either directly or through an intermediary, to any County officer, employee or agent with the intent of securing this Agreement or securing favorable treatment with respect to the award, Amendment or extension of the Agreement or the making of any determinations with respect to Contractor's performance pursuant to this Agreement. In the event of such termination, County shall be entitled to pursue the same remedies against Contractor as it could pursue in the event of default by Contractor.
- 22.2 Contractor shall immediately report any attempt by a County officer or employee to solicit such improper consideration. The report shall be made either to County manager charged with the supervision of the employee or to County's Auditor-Controller Employee Fraud Hotline at (213) 974 0914 or (800) 544 6861.
- 22.3 Among other items, such improper consideration may take the form of cash, discounts, services, the provision of travel or entertainment, or tangible gifts.

23. TERMINATION FOR INSOLVENCY

- 23.1 County may terminate this Agreement immediately at any time upon the occurrence of any of the following:
- (1) Insolvency of Contractor. Contractor shall be deemed to be insolvent if it has ceased to pay or has admitted in writing its inability to pay its debts for at least sixty (60) days in the ordinary course of business or cannot pay its debts as they become due, whether or not a petition has been filed under the United States Bankruptcy Code and whether or not Contractor is insolvent within the meaning of the United States Bankruptcy Code, provided that Contractor shall not be deemed insolvent if it has ceased in the normal course of business to pay its debts which are disputed in good faith and which are not related to this Agreement as determined by County;
 - (2) The filing of a voluntary or involuntary petition to have Contractor declared bankrupt, where the involuntary petition is not dismissed within sixty (60) days;
 - (3) The appointment of a receiver or trustee for Contractor; or
 - (4) The execution by Contractor of an assignment for the benefit of creditors.

- 23.2 The rights and remedies of County provided in this Paragraph 23 shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Agreement.
- 23.3 Contractor agrees that if Contractor as a debtor-in-possession, or if a trustee in bankruptcy, rejects this Agreement, County may elect to retain its rights under this Agreement, as provided under Section 365(n) of the United States Bankruptcy Code (11 United States Code, Section 365(n)). Upon written request of County to Contractor or the trustee in bankruptcy, as applicable, Contractor or such trustee shall allow County to exercise all of its rights and benefits under this Agreement including, without limitation, such Section 365(n) (including, without limitation, the right to continued use of all source and object code versions of the Application Software and related Documentation in accordance with the terms of Paragraph 10.3 (Source Code) and the Source Code Agreement, and shall not interfere with the rights and benefits of County as provided therein. The foregoing shall survive the termination or expiration of this Agreement for any reason whatsoever.

24. EFFECT OF TERMINATION

In the event that County, upon thirty (30) days' written notice to Contractor, terminates this Agreement in whole or in part as provided herein, then:

- (1) Contractor and County shall continue the performance of this Agreement to the extent not terminated;
- (2) Contractor shall stop Work under this Agreement on the date and to the extent specified in such written notice and provide to County all County Materials and County owned Work in progress, in a media reasonably requested by County;
- (3) Contractor shall promptly return to County any and all County deemed Confidential Information, including County data and County Materials, that relate to that portion of the Agreement and Work terminated by County;
- (4) County shall pay Contractor all monies due in accordance with the terms of the Agreement and the Statement of Work for the Work completed up to the time of termination;
- (5) Contractor shall return to County all monies paid by County, yet unearned by Contractor, including any prorated prepaid Service Fees calculated depending on the date of termination, if applicable;
- (6) Upon termination by County for default pursuant to Paragraph 20 (Termination for Default) or for insolvency pursuant to Paragraph 23 (Termination for Insolvency), County shall have the right to procure goods, services and other work, similar to those so terminated, and Contractor shall be liable to County for, and shall promptly pay to County by cash payment, excess costs incurred by County to procure and furnish such similar goods, services and other work;
- (7) County shall have the rights set forth in Paragraphs 10.2 (License) and 10.3 (Source Code) to access and use the Application Software Source Code as set forth therein, including without limitation the right to modify all source and object code versions of the Application Software only after such time as one of the Release Conditions described in Paragraph 10.3.3 (Source Code Release Conditions) has occurred which would permit County to use the Source Code in accordance with the terms of Paragraph 10.2 (License);

- (8) Upon termination by County for convenience pursuant to Paragraph 21) Termination for Convenience) during the Initial Term, County will pay Contractor a pro-rata portion of Contractor's initial investment as provided in Paragraph 21.3 above; and
- (9) Contractor understands and agrees that County has obligations that it cannot satisfy without use of the System provided to County hereunder or an equivalent solution, and that a failure to satisfy such obligations could result in irreparable damage to County and the entities it serves. Therefore, Contractor agrees that in the event of any termination of this Agreement, Contractor shall reasonably and in accordance with industry standards cooperate with County in the transition of County to a new solution, toward the end that there be no interruption of County's day to day operations due to the unavailability of the System during such transition. Upon written notice to Contractor, Contractor shall allow County or another selected contractor a reasonable transition period, as mutually agreed upon by the Parties, for the orderly turnover of Contractor's Agreement activities and responsibilities without additional cost to County.

25. INDEPENDENT CONTRACTOR STATUS

- 25.1 This Agreement is not intended to, and shall not be construed to, create the relationship of agent, servant, employee, partnership, joint venture or association as between County and Contractor. The employees and agents of one party are not and shall not be, or construed to be, the employees or agents of the other party for any purpose whatsoever. Contractor shall function as, and in all respects is, an independent Contractor.
- 25.2 Contractor shall be solely liable and responsible for providing all workers' compensation insurance and benefits, liability insurance, employer taxes, compensation and benefits to, or on behalf of, all persons performing Work pursuant to this Agreement. County shall have no liability or responsibility for the payment of any salaries, wages, unemployment benefits, payroll taxes, disability insurance or benefits, or Federal, State or local taxes, or other compensation, benefits or taxes for any personnel provided by or performing Work on behalf of Contractor.
- 25.3 The employees and agents of Contractor shall, while on the premises of County, comply with all rules and regulations of the premises, including, but not limited to, security requirements.
- 25.4 Notwithstanding the provisions of this Paragraph 25, the employees and agents of Contractor shall, while on the premises of County, comply with all rules and regulations of the premises, including, but not limited to, security requirements.

26. SUBCONTRACTING

- 26.1 County has relied, in entering into this Agreement, on the reputation of and on obtaining the personal performance of Contractor, specifically, Contractor Key Staff. Consequently, no performance by the Contractor Key Staff of this Agreement, or any portion thereof, shall be subcontracted by Contractor without notice to County as provided in this Paragraph 26. Any attempt by Contractor to subcontract any performance of this Agreement by the Contractor Key Staff without such notice shall be null and void and shall be deemed a material breach of this Agreement, upon which County may immediately terminate this Agreement.
- 26.2 In the event Contractor subcontracts any portion of its performance of the Agreement by the Contractor Key Staff, Contractor shall provide to County, in writing, a notice regarding such subcontract, which shall include:

- (1) The reasons for the particular subcontract;
- (2) Identification of the proposed subcontractor and an explanation of why and how the proposed subcontractor was selected;
- (3) A detailed description of the Work to be provided by the proposed subcontractor;
- (4) Confidentiality provisions applicable to the proposed subcontractor's officers, employees and agents, which would be incorporated into the subcontract;
- (5) include (i) Exhibit F (Confidentiality and Assignment Agreement), (ii) Exhibit G (Contractor's EEO Certification), (iii) Exhibit I (Safely Surrendered Baby Law), and (iii) any other standard County required provisions;
- (6) A representation from Contractor that:
 - a. the proposed subcontractor is qualified to provide the Work for which subcontractor is being hired;
 - b. either the proposed subcontractor maintains the insurance required by this Agreement or Contractor has procured and maintains such insurance coverage for the proposed subcontractor;
 - c. either the proposed subcontractor or Contractor shall be solely liable and responsible for any and all of subcontractor's taxes, payments and compensation, including compensation to its employees, related to the performance of Work under this Agreement; and
 - d. either the proposed subcontractor or Contractor shall provide for indemnification of County under the same terms and conditions as the indemnification provisions of this Agreement, including those specified in Paragraphs 13 (Indemnification) and 15 (Intellectual Property Warranty and Indemnification); and
- (7) Other pertinent information and/or certifications reasonably requested by County.

26.3 County will review Contractor's request to subcontract and determine on a case-by-case basis whether or not to consent to such request, which consent shall not be unreasonably withheld.

26.4 Notwithstanding any provision of this Agreement to the contrary, whether expressly or by implication, Contractor shall indemnify, defend and hold harmless County, its officers, employees and agents, from and against any and all claims, demands, liabilities, damages, costs and expenses, including, but not limited to, defense costs and legal, accounting or other expert consulting or professional fees in any way arising from or related to Contractor's use of any subcontractor, including, without limitation, any officers, employees or agents of any subcontractor, in the same manner as required for Contractor, its officers, employees and agents, under this Agreement.

26.5 Notwithstanding any other provision of this Paragraph 26, Contractor shall remain fully responsible for any and all performance required of it under this Agreement, including those which Contractor has determined to subcontract, including, but not limited to, the obligation to properly supervise, coordinate and provide all Work required under this Agreement. All subcontracts shall be made in the name of Contractor and shall not bind nor purport to bind County. Furthermore, subcontracting of any Work under this Agreement shall not be construed to limit, in any way, Contractor's performance, obligations or responsibilities to County or limit, in any way, any of County's rights or remedies contained in this Agreement.

26.6 Subcontracting of any Work performed by the Contractor Key Staff under the Agreement shall not waive County's right to prior and continuing approval of any or all such Contractor Key Staff pursuant to the provisions of Paragraph 3.3 (Approval of Contractor's Staff), including any subcontracted members of the Contractor Key Staff. Contractor shall notify its subcontractors of this County's right prior to subcontractors commencing performance under this Agreement.

26.7 Notwithstanding subcontracting by Contractor of any Work under this Agreement, Contractor shall be solely liable and responsible for any and all payments and other compensation to all subcontractors, and their officers, employees, agents, and successors in interest, for any services performed by subcontractors under this Agreement.

26.8 In the event that County consents to any subcontracting, such consent shall apply to each particular subcontract only and shall not be, or be construed to be, a waiver of this Paragraph 26 or a blanket consent to any further subcontracting.

27. RISK OF LOSS

Contractor shall bear the full risk of loss due to total or partial destruction of any Software products loaded on CDs or other computer media, until such items are delivered to and accepted in writing by County as evidenced by County's signature on delivery documents.

28. MOST FAVORED PUBLIC ENTITY

If Contractor's prices decline, or should Contractor, at any time during the term of this Agreement, provide similar software, service levels, software models, components, goods or services under similar terms and conditions to the State of California or any county, municipality, or district of the State or to any other state, county or municipality at prices below those set forth in this Agreement, then such lower prices shall be immediately extended to County. Any information provided by Contractor pursuant to the provisions of this Paragraph 28 (i) that is not public and (ii) that is deemed as proprietary and confidential by Contractor shall be treated by County as Contractor's Confidential Information to the extent permissible by law, provided that Contractor provides County an advance written notice as to such designation. Notwithstanding the foregoing, such pricing information shall be subject to California Public Records Act.

29. RECORDS AND AUDITS

29.1 Contractor shall maintain accurate and complete financial records of its activities and operations relating to this Agreement in accordance with generally accepted accounting principles. Contractor agrees that County, or its authorized representatives, shall have access to and the right to examine, audit, excerpt, copy, or transcribe any pertinent transaction, activity, or records relating to this Agreement to the extent required by law. All such material shall be kept and maintained by Contractor during the term of this Agreement and for a period of five (5) years thereafter, unless County's written permission is given to dispose of any such material prior to such time. All such material shall be maintained by Contractor at a location in Los Angeles County, provided that if any such material is located outside Los Angeles County, Contractor shall make the necessary arrangements at its own cost and expense to have such material made available to the County within County's borders.

29.2 In the event that an audit is conducted of Contractor specifically regarding this Agreement by any Federal or State auditor, then Contractor shall file a copy of such audit report with

County's Auditor-Controller within thirty (30) days of Contractor's receipt thereof, unless otherwise provided by applicable Federal or State law or under this Agreement. County shall make a reasonable effort to maintain the confidentiality of such audit report(s).

- 29.3 Failure on the part of Contractor to comply with any of the provisions of this Paragraph 29 shall constitute a breach of this Agreement upon which County may terminate or suspend this Agreement under the terms of Paragraph 20 (Termination for Default).

30. COUNTY'S QUALITY ASSURANCE PLAN

County, or its agent, will evaluate Contractor's performance under this Agreement on not less than an annual basis. Such evaluation will include assessing Contractor's compliance with the terms and conditions of this Agreement. Contractor deficiencies, which County determines are severe or continuing and that may place performance of this Agreement in jeopardy, if not corrected, will be reported to the County's Board of Supervisors. The report will include improvements and/or corrective action measures taken by County and Contractor. If improvement does not occur consistent with the corrective action measures within thirty (30) days of County's notice of Contractor deficiencies, County may, at its sole option, terminate this Agreement, in whole or in part, pursuant to Paragraph 20 (Termination for Default) or Paragraph 21 (Termination for Convenience), or impose other penalties as specified in this Agreement.

31. CONFLICT OF INTEREST

- 31.1 No County employee whose position with County enables such employee to influence the award of this Agreement or any competing agreements shall be employed in any capacity by Contractor or have any other direct financial interest in this Agreement. No officer or employee of Contractor, who may financially benefit from the performance of Work hereunder, shall in any way participate in County's approval or ongoing evaluation of such Work, or in any way attempt to unlawfully influence County's approval or ongoing evaluation of such work.
- 31.2 Contractor shall comply with all conflict of interest laws, ordinances and regulations now in effect or hereafter to be enacted during the term of this Agreement which are applicable to it as a software and services provider. Contractor warrants that it is not now aware of any facts which do create an unlawful conflict of interest for Contractor. If a party hereafter becomes aware of any facts, which might reasonably be expected to create an unlawful conflict of interest for it, it shall immediately make full written disclosure of such facts to County. Full written disclosure shall include, but is not limited to, identification of all persons implicated and a complete description of all relevant circumstances.

32. COMPLIANCE WITH APPLICABLE LAWS

- 32.1 In the performance of this Agreement, Contractor shall comply with all applicable Federal, State, and local laws, rules, regulations, ordinances, directives, guidelines, policies, and procedures, and all provisions required thereby to be included in this Agreement are hereby incorporated herein by reference.
- 32.2 Contractor shall indemnify, defend and hold harmless County, its elected and appointed officers, employees, and agents, from and against any and all claims, demands, damages, liabilities, losses, costs, and expenses, including, without limitation, defense costs and legal, accounting and other expert, consulting or professional fees, arising from, connected with, or related to any failure by Contractor, its officers, employees, agents or subcontractors, to

comply with any such applicable laws, rules, regulations, ordinances, directives, guidelines, policies, or procedures. Any legal defense pursuant to Contractor's indemnification obligations under this Paragraph 32 shall be conducted by Contractor and performed by counsel selected by Contractor and approved by County. Notwithstanding the preceding sentence, County shall have the right to participate in any such defense at its sole cost and expense, except that in the event Contractor fails to provide County with full and adequate defense, as determined by County in its sole judgment, County shall be entitled to retain its own counsel, including without limitation, County Counsel, and reimbursement from Contractor for all such costs and expenses incurred by County in doing so. Contractor shall not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

- 32.3 Contractor certifies and agrees that it fully complies with all applicable requirements of the applicable County regulations, as well as applicable rules, ordinances, court rules, municipal laws, directives and policies issued pursuant to the enabling statute(s) and/or State or Federal regulation or law. This includes compliance with mandatory standards and policies relating to energy efficiency in the State Energy Conservation Plan (Title 24, California Administrative Code), the Energy Policy and Conservation Act (Pub. L. 94-163, 89 Stat. 871) and compliance with Section 306 of the Clean Air Act (42 USC 1857[h]), Section 508 of the Clean Water Act (33 USC 1368), Executive Order 11738 and Environmental Protection Agency regulations (40 CFR Part 15). Contractor shall be responsible for any relevant changes in the law, including but not limited to, changes in County regulations, rules, ordinances, court rules, municipal laws, directives and policies issued pursuant to the enabling statute(s) and/or State or Federal regulation or law. Contractor shall also comply with all applicable ordinances, rules, policies, directives, and procedures issued or adopted by County for which Contractor is provided actual or constructive notice. County reserves the right to review Contractor's procedures to ensure compliance with the statutes, ordinances, regulations, rules, rulings, policies and procedures of the State and the Federal government, as applicable.
- 32.4 Failure by Contractor to comply with such laws and regulations shall be material breach of this Agreement and may result in termination of this Agreement.

33. FAIR LABOR STANDARDS

Contractor shall comply with all applicable provisions of the Federal Fair Labor Standards Act, and shall indemnify, defend, and hold harmless County, its elected and appointed officers, and employees from any and all third party liability for, wages, overtime pay, liquidated damages, penalties, court costs and attorneys' fees arising from acts engaged in by Contractor in violation of applicable wage and hour laws in the State of California and in the Federal Fair Labor Standards Act, for work performed by Contractor's employees for which County may be found jointly or solely liable, provided that County: (i) promptly notifies Contractor in writing of the claim; and (ii) allows Contractor to control, and cooperate with Contractor in, the defense and any related settlement negotiations.

34. COMPLIANCE WITH CIVIL RIGHTS LAWS

- 34.1 Contractor herein certifies and agrees, and will re-certify upon County request no more frequently than once per year, that all persons employed by it, its affiliates, subsidiaries and holding companies will be treated equally without regard to or because of race, color,

religion, ancestry, national origin, sex, age, physical or mental handicap, marital status or political affiliation, in compliance with all applicable Federal and State anti-discrimination laws and regulations.

34.2 Contractor shall, pursuant to Los Angeles County Code Section 4.32, certify to and comply with the provisions of Contractor's EEO Certification (Exhibit G).

34.3 Contractor shall ensure that applicants and employees are treated equally during employment, without regard to race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status or political affiliation, in compliance with all applicable Federal and State anti-discrimination laws and regulations. Such action shall include, but is not limited to: employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

34.4 Contractor herein certifies and agrees, and will re-certify upon County request no more frequently than once per year, that it will deal with its subcontractors, bidders or vendors without regard to or because of race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status or political affiliation, except to the extent necessary to comply with applicable Federal and State anti-discrimination laws and regulations.

34.5 Contractor herein certifies, and will re-certify upon County request no more frequently than once per year, that it, its affiliates, subsidiaries and holding companies are in compliance with all Federal, State, and local laws including, but not limited to:

(1) Title VII, Civil Rights Act of 1964;

(2) Section 504, Rehabilitation Act of 1973;

(3) Age Discrimination Act of 1975;

(4) Title IX, Education Amendments of 1973, as applicable; and

(5) Title 43, Part 17, Code of Federal Regulations, Subparts A & B,

and that no person shall, on the grounds of race, creed, color, national origin, political affiliation, marital status, sex, age, or disability, be subject to discrimination as to any privileges or uses gained under this Agreement or under any project, program or activity supported by this Agreement.

34.6 Contractor shall allow County representatives access to Contractor's employment records during regular business hours to verify compliance with the provisions of this Paragraph 34 when so requested by County with no less than ten (10) days' advance written notice.

34.7 If County finds that any of the provisions of this Paragraph 34 have been violated, such violation shall, at the election of County, constitute a material breach of this Agreement upon which County may terminate or suspend this Agreement at County's option, either for material breach under Paragraph 20 (Termination for Default) of this Agreement or for convenience under Paragraph 21 (Termination for Convenience) of this Agreement. While County reserves the right to determine independently that the anti-discrimination provisions of this Agreement have been violated, in addition, a determination by the California Fair Employment Practices Commission or the Federal Equal Employment Opportunity Commission that Contractor has violated State or Federal anti-discrimination laws or

regulations shall constitute a finding by County that Contractor has violated the anti-discrimination provisions of this Agreement.

- 34.8 The parties agree that in the event Contractor is found to have violated the anti-discrimination provisions of this Agreement, and that such discrimination was directly associated with the performance of services provided under this Agreement, County may require, pursuant to Los Angeles County Code Section 4.32.010 (E), that Contractor pay the sum of Five hundred Dollars (\$500) for each such violation, in lieu of termination or suspension hereof, as liquidated damages are extremely difficult to ascertain or calculate precisely. In the alternative, County may elect to terminate this Agreement pursuant to Paragraph 20 (Termination for Default).

35. RESTRICTIONS ON LOBBYING

35.1 FEDERAL FUNDS PROJECTS

If any Federal funds are to be used to pay for any portion of Contractor's Work under this Agreement, County shall notify Contractor in writing in advance of such payment and Contractor shall fully comply with all certification and disclosure requirements prescribed by Section 319 of Public law 101-121 (31 United States Code Section 1352) and any implementing regulations, and shall ensure that each of its subcontractors receiving funds provided under this Agreement also fully complies with all applicable certification and disclosure requirements.

35.2 LOBBYIST ORDINANCE

Contractor, and each County lobbyist or County lobbying firm, as defined in Los Angeles County Code Section 2.160.010, retained by Contractor, shall fully comply with County's Lobbyist Ordinance, Los Angeles County Code Chapter 2.160. Failure on the part of Contractor or any County lobbyist or County lobbying firm retained by Contractor to fully comply with County Lobbyist Ordinance shall constitute a material breach of this Agreement, upon which County may immediately terminate or suspend this Agreement at County's option, either for material breach under Paragraph 20 (Termination for Default) of this Agreement or for convenience under Paragraph 21 (Termination for Convenience) of this Agreement.

36. EMPLOYMENT ELIGIBILITY VERIFICATION

- 36.1 Contractor warrants that it fully complies with all Federal and State statutes and regulations regarding employment of aliens and others and that all its employees performing Services under this Agreement meet the citizenship or alien status requirements contained in Federal and State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986 (P.L. 99-603).
- 36.2 Contractor shall obtain from all employees performing under this Agreement all verification and other documentation of employment eligibility status required by Federal statutes and regulations as they currently exist and as they may be hereafter amended. Contractor shall retain such documentation for the period prescribed by law.
- 36.3 Contractor shall indemnify, defend, and hold harmless County, its officers, employees and agents from and against any and all claims, demands, damages, liabilities, losses, costs, and expenses, including, but not limited to, defense costs and legal, accounting and other expert, consulting or professional fees, arising out of or in connection with any employer sanctions

and any other liability which may be assessed against Contractor or County in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing Work under this Agreement.

37. CONTRACT HIRING

37.1 CONSIDERATION OF HIRING COUNTY EMPLOYEES TARGETED FOR LAYOFFS

Should Contractor require additional or replacement personnel after the effective date of this Agreement to perform the Work set forth herein, Contractor shall give first consideration for such employment openings to permanent County employees who are targeted for layoff or qualified former County employees who are on a re-employment list during the term of this Agreement.

37.2 CONSIDERATION OF GAIN/GROW PROGRAM PARTICIPANTS FOR EMPLOYMENT

Should Contractor require additional or replacement personnel after the Effective Date, Contractor shall give consideration for any such employment openings to participants in the County's Department of Public Social Services' Greater Avenues for Independence (GAIN) Program or General Relief Opportunity for Work (GROW) Program who meet Contractor's minimum qualifications for the open position. For this purpose, consideration shall mean that Contractor will interview qualified candidates. County will refer GAIN participants by job category to Contractor.

In the event that both laid-off County employees and GAIN/GROW participants are available for hiring, Contractor shall give County employees first priority.

37.3 PROHIBITION AGAINST INDUCEMENT AND PERSUASION

Contractor and County agree that, during the term of this Agreement and for a period of one (1) year thereafter, neither party shall in any way intentionally induce or persuade any employee of one party to become an employee or agent of the other party. Notwithstanding the foregoing, such prohibition shall not apply to any hiring action initiated through a public announcement.

38. FEDERAL EARNED INCOME CREDIT

If required by applicable law, Contractor shall notify its employees, and shall require each subcontractor to notify its employees, that they may be eligible for the Federal Earned Income Credit under the Federal income tax laws. Such notice shall be provided, in accordance with the requirements set forth in Internal Revenue Service Notice 1015.

39. CONTRACTOR RESPONSIBILITY AND DEBARMENT

39.1 RESPONSIBLE CONTRACTOR

A responsible contractor is a contractor who has demonstrated the attribute of trustworthiness, as well as quality, fitness, capacity and experience to satisfactorily perform the Agreement. It is County's policy to conduct business only with responsible contractors.

39.2 CHAPTER 2.202

Contractor is hereby notified that, in accordance with Chapter 2.202 of the Los Angeles Code, if County acquires information concerning the performance of Contractor on this Agreement or other contracts which indicates that Contractor is not responsible, County may,

in addition to other remedies provided in this Agreement, debar Contractor from bidding or proposing on, or being awarded, and/or performing Work on, County agreements for a specified period of time, which generally will not exceed five (5) years, although may exceed five (5) years or be permanent if warranted by the circumstances, and terminate any or all existing agreements Contractor may have with County.

39.3 NON-RESPONSIBLE CONTRACTOR

County may debar Contractor if County's Board of Supervisors finds, in its discretion, that Contractor has done any of the following: (i) violated any term of a contract with County or a nonprofit corporation created by County; (ii) committed any act or omission which negatively reflects on Contractor's quality, fitness or capacity to perform a contract with County, any other public entity or a nonprofit corporation created by County, or engaged in a pattern or practice which negatively reflects on same; (iii) committed an act or offense which indicates a lack of business integrity or business honesty; or (iv) made or submitted a false claim against County or any other public entity.

39.4 CONTRACTOR HEARING BOARD

39.4.1 If there is evidence that Contractor may be subject to debarment, County's Project Director, or his/her designee, will notify Contractor in writing of the evidence which is the basis for the proposed debarment and will advise Contractor of the scheduled date for a debarment hearing before County's Contractor Hearing Board.

39.4.2 The Contractor Hearing Board will conduct a hearing where evidence on the proposed debarment is presented. Contractor and/or Contractor's representative shall be given an opportunity to submit evidence at that hearing. After the hearing, the Contractor Hearing Board will prepare a tentative proposed decision, which shall contain a recommendation regarding whether Contractor should be debarred, and, if so, the appropriate length of time of the debarment. Contractor, County's Project Director, or his/her designee, and County's departments shall be provided with an opportunity to object to the tentative proposed decision prior to its presentation to County's Board of Supervisors.

39.4.3 After consideration of any objections, or if no objections are submitted, a record of the hearing, the proposed decision and any other recommendation of the Contractor Hearing Board shall be presented to County's Board of Supervisors. The Board of Supervisors shall have the right to modify, deny or adopt the proposed decision and recommendation of the Contractor Hearing Board.

39.4.4 If Contractor has been debarred for a period longer than five (5) years, then Contractor may, after the debarment has been in effect for at least five (5) years, submit a written request for review of the debarment determination to reduce the period of debarment or terminate the debarment. County may, in its discretion, reduce the period of debarment or terminate the debarment if it finds that such Contractor has adequately demonstrated one or more of the following: (i) elimination of the grounds for which the debarment was imposed; (ii) a bona fide change in ownership or management; (iii) material evidence discovered after debarment was imposed; or (iv) any other reason that is in the best interests of County.

39.4.5 The Contractor Hearing Board will consider a request for review of a debarment determination only where (i) the requesting contractor has been debarred for a period longer than five (5) years, (ii) the debarment has been in effect for at least five (5) years and (iii) the request is in writing, states one or more of the grounds for reduction of the debarment period

or termination of the debarment, and includes supporting documentation. Upon receiving an appropriate request, the Contractor Hearing Board will provide notice of the hearing on the request. At the hearing, the Contractor Hearing Board shall conduct a hearing where evidence on the proposed reduction of debarment period or termination of debarment is presented. This hearing shall be conducted and the request for review decided by the Contractor Hearing Board pursuant to the same procedures as for a debarment hearing.

- 39.4.6 The Contractor Hearing Board's proposed decision shall contain a recommendation on the request to reduce the period of debarment or terminate the debarment. The Contractor Hearing Board shall present its proposed decision and recommendation to County's Board of Supervisors. County's Board of Supervisors shall have the right to modify, deny, or adopt the proposed decision and recommendation of the Contractor Hearing Board.

39.5 **SUBCONTRACTORS OF CONTRACTOR**

The terms and procedures of this Paragraph 39 shall also apply to subcontractors, consultants and partners of Contractor performing Work under this Agreement.

40. **FEDERAL ACCESS TO RECORDS**

If, and to the extent that Section 1861(v)(1)(I) of the Social Security Act (42 United States Code Section 1395x(v)(1)(i) is applicable, Contractor agrees that for a period of four (4) years following the furnishing of services under this Agreement, Contractor shall maintain and make available, upon written request, to the Secretary of the United States Department of Health and Human Services or the Comptroller General of the United States or to any of their authorized representatives, the contracts, books, documents and records of Contractor which are necessary to verify the nature and extent of the costs of services provided hereunder. Furthermore, if Contractor carries out any of the services described in 42 United States Code Section 1395 through any subcontract with a value or cost of Ten Thousand Dollars (\$10,000) or more over a twelve month period with a related organization (as that term is defined under Federal law), Contractor agrees that each such subcontract shall provide for such access to the subcontract, books, documents and records of the subcontractor.

41. **REQUIRED CERTIFICATIONS**

Contractor shall obtain and maintain in effect during the term of this Agreement all licenses, permits, registrations, accreditations and certificates required by all Federal, State, and local laws, ordinances, rules, regulations, guidelines and directives, which are applicable to Contractor's provision of the Services under this Agreement. Contractor shall further ensure that all of its officers, employees, agents and subcontractors who perform Services hereunder, shall obtain and maintain in effect during the term of this Agreement all licenses, permits, registrations, accreditations and certificates which are applicable to their performance hereunder. A copy of each such license, permit, registration, accreditation and certificate required by all applicable Federal, State, and local laws, ordinances, rules, regulations, guidelines and directives shall be provided, if required by law, in duplicate, to County's Project Manager at the address set forth in Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement).

42. **NO THIRD PARTY BENEFICIARIES**

Notwithstanding any other provision of this Agreement, Contractor and County do not in any way intend that any person or entity shall acquire any rights as a third party beneficiary of

this Agreement, except that this provision shall not be construed to diminish Contractor's indemnification obligations hereunder.

43. CONTRACTOR PERFORMANCE DURING CIVIL UNREST AND DISASTER

Contractor recognizes that County provides services essential to the residents of the communities it serves, and that these services are of particular importance at the time of a riot, insurrection, civil unrest, natural disaster or similar event. Notwithstanding any other provision of this Agreement, full performance by Contractor during any riot, insurrection, civil unrest, natural disaster or similar event is not excused if such performance remains physically possible without related danger to Contractor's or subcontractors' employees and suppliers. During any such event in which the health or safety of any of Contractor's staff members would be endangered by performing their services on-site, such staff members may perform any or all of their services remotely.

44. WARRANTY AGAINST CONTINGENT FEES

44.1 Contractor warrants that no person or selling agency has been employed or retained to solicit or secure this Agreement upon any agreement or understanding for a commission, percentage, brokerage, or contingent fee, excepting bona fide employees or bona fide established commercial or selling agencies maintained by Contractor for the purpose of securing business.

44.2 For breach of this warranty, County shall have the right to terminate this Agreement and, at its sole discretion, deduct from the fees owed, or otherwise recover, the full amount of such commission, percentage, brokerage, or contingent fee.

45. SAFELY SURRENDERED BABY LAW

45.1 NOTICE

As required by applicable law, Contractor shall notify and provide to its employees, and shall require each subcontractor to notify and provide to its employees, a fact sheet regarding the Safely Surrender Baby Law, its implementation in Los Angeles County, and where and how to safely surrender a baby. The fact sheet is available on the Internet at <http://babysafela.org> for printing purposes.

45.2 ACKNOWLEDGMENT OF COMMITMENT

Contractor acknowledges that County places a high priority on the implementation of the Safely Surrendered Baby Law. Contractor understands that it is County's policy to encourage all County Contractors to voluntarily post County's "Safely Surrendered Baby Law" poster in a prominent position at Contractor's place of business. Contractor will also encourage its subcontractors, if any, to post this poster in a prominent position in the subcontractor's place of business. County's Department of Children and Family Services will supply Contractor with the poster to be used.

46. COMPLIANCE WITH COUNTY'S JURY SERVICE PROGRAM

46.1 JURY SERVICE PROGRAM

This Agreement is subject to the provisions of County's ordinance entitled Contractor Employee Jury Service Program (hereinafter "Jury Service Program" or "Program") as codified in Sections 2.203.010 through 2.203.090 of the Los Angeles County Code (hereinafter "County Code").

46.2 WRITTEN EMPLOYEE JURY SERVICE POLICY

- 46.2.1 Unless Contractor has demonstrated to County's satisfaction either that Contractor is not a "Contractor" as defined under the Jury Service Program (Section 2.203.020 of the County Code) or that Contractor qualifies for an exception to the Jury Service Program (Section 2.203.070 of the County Code), Contractor shall have and adhere to a written policy that provides that its Employees (as defined in Paragraph 46.2.2 below) shall receive from Contractor, on an annual basis, no less than five (5) days of regular pay for actual jury service. The policy may provide that Employees deposit any fees received for such jury service with Contractor or that Contractor deduct from the Employee's regular pay the fees received for jury service.
- 46.2.2 For purposes of this Paragraph 46, "Contractor" means a person, partnership, corporation or other entity which has an agreement with County or a subcontract with Contractor and has received or will receive an aggregate sum of \$50,000 or more in any twelve (12) month period under one or more County agreements or subcontracts. "Employee" means any California resident who is a full time employee of Contractor. "Full time" means forty (40) hours or more worked per week, or a lesser number of hours if: 1) the lesser number is a recognized industry standard as determined by County, or 2) Contractor has a longstanding practice that defines the lesser number of hours as fulltime. Fulltime employees providing short term, temporary services of ninety (90) days or less within a twelve (12) month period are not considered fulltime for purposes of the Jury Service Program. If Contractor uses any subcontractor to perform services for County under this Agreement, the subcontractor shall also be subject to the provisions of this Paragraph 46. The provisions of this Paragraph 46 shall be inserted into any such subcontract and a copy of the Jury Service Program shall be attached to the agreement.
- 46.2.3 If Contractor is not required to comply with the Jury Service Program when the Agreement commences, Contractor shall have a continuing obligation to review the applicability of its "exception status" from the Jury Service Program, and Contractor shall immediately notify County if Contractor at any time either comes within the Jury Service Program's definition of "Contractor" or if Contractor no longer qualifies for an exception to the Program. In either event, Contractor shall immediately implement a written policy consistent with the Jury Service Program. County may also require, at any time during this Agreement and at its sole discretion, that Contractor demonstrate to County's satisfaction that Contractor either continues to remain outside of the Jury Service Program's definition of "Contractor" and/or that Contractor continues to qualify for an exception to the Program.
- 46.2.4 Contractor's violation of this Paragraph 46 of this Agreement may constitute a material breach of the Agreement. In the event of such material breach, County may, in its sole discretion, terminate this Agreement with Contractor and/or bar Contractor from the award of future County agreements for a period of time consistent with the seriousness of the breach.

47. CONTRACTOR'S WARRANTY OF ADHERENCE TO COUNTY'S CHILD SUPPORT COMPLIANCE PROGRAM

- 47.1 Contractor acknowledges that County has established a goal of ensuring that all individuals who benefit financially from County through County agreements are in compliance with their court ordered child, family and spousal support obligations in order to mitigate the economic burden otherwise imposed upon County and its taxpayers.

47.2 As required by County's Child Support Compliance Program (County Code Chapter 2.200) and without limiting Contractor's duty under this Agreement to comply with all applicable provisions of State and Federal law, Contractor warrants that to the best of its knowledge it is now in compliance and shall during the term of this Agreement maintain compliance with employment and wage reporting requirements as required by the Federal Social Security Act (42 USC Section 653(a)) and California Unemployment Insurance Code Section 1088.5, and shall, implement all lawfully served Wage and Earnings Withholding Orders or County's Child Support Services Department Notices of Wage and Earnings Assignment for Child or Spousal Support, pursuant to Code of Civil Procedure Section 706.031 and Family Code Section 5246(b).

48. TERMINATION FOR BREACH OF WARRANTY TO MAINTAIN COMPLIANCE WITH COUNTY'S CHILD SUPPORT COMPLIANCE PROGRAM

Failure of Contractor to maintain compliance with the requirements set forth in Paragraph 47 (Contractor's Warranty of Adherence to County's Child Support Compliance Program) shall constitute a default by Contractor under this Agreement. Without limiting the rights and remedies available to County under any other provision of this Agreement, failure to cure such default within ninety (90) days of notice by County's Child Support Services Department shall be grounds upon which the Auditor-Controller or County's Board of Supervisors may terminate this Agreement pursuant to Paragraph 20 (Termination for Default) and pursue debarment of Contractor pursuant to Paragraph 39 (Contractor Responsibility and Debarment).

49. CHARITABLE ACTIVITIES COMPLIANCE [IF APPLICABLE]

The Supervision of Trustees and Fundraisers for Charitable Purposes Act regulates entities receiving or raising charitable contributions. The "Nonprofit Integrity Act of 2004" (SB 1262, Chapter 919) increased Charitable Purposes Act requirements. Contractor shall complete the certification in Exhibit J (Charitable Contributions Certification). By requiring contractors to complete the certification in Exhibit J (Charitable Contributions Certification), County seeks to ensure that all County contractors which receive or raise charitable contributions comply with the California law in order to protect County and its taxpayers. By receiving or raising charitable contributions without complying with its obligations under California law, Contractor commits a material breach of this Agreement, subjecting it to either Agreement termination or debarment proceedings or both (County Code Chapter 2.202).

50. DEFAULTED PROPERTY TAX REDUCTION PROGRAM

50.1 CONTRACTOR'S WARRANTY OF COMPLIANCE WITH COUNTY'S DEFAULTED PROPERTY TAX REDUCTION PROGRAM

Contractor acknowledges that County has established a goal of ensuring that all individuals and businesses who benefit financially from County through contract are current in paying their property tax obligations (secured and unsecured roll) in order to mitigate the economic burden otherwise imposed upon County and its taxpayers.

Unless Contractor qualifies for an exemption or exclusion, Contractor warrants and certifies that to the best of its knowledge it is now in compliance, and during the term of this Agreement will maintain compliance, with Los Angeles County Code Chapter 2.206.

50.2 TERMINATION FOR BREACH OF WARRANTY TO MAINTAIN COMPLIANCE WITH COUNTY'S DEFAULTED PROPERTY TAX REDUCTION PROGRAM

Failure of Contractor to maintain compliance with the requirements set forth in Paragraph 50.1 (Contractor's Warranty of Compliance with County's Defaulted Property Tax Reduction Program) shall constitute default under this Agreement. Without limiting the rights and remedies available to County under any other provision of this Agreement, failure of Contractor to cure such default within ten (10) days of notice shall be grounds upon which County may terminate this Agreement and/or pursue debarment of Contractor pursuant to County Code Chapter 2.206.

51. COUNTY AUDIT SETTLEMENTS

If, at any time during or after the term of this Agreement, representatives of County conduct an audit of Contractor regarding the Work performed under this Agreement, and if such audit reasonably and accurately find that County's dollar liability for such work is less than payments made by County to Contractor, then the difference, together with County's reasonable costs of audit, shall be either repaid by Contractor to County by cash payment upon demand or deducted from any amounts due to Contractor from County, as determined by County. If such audit finds County's dollar liability for such Work is more than payments made by County to Contractor, then the difference shall be repaid to Contractor by cash payment.

52. DISPUTE RESOLUTION PROCEDURE

- 52.1 Contractor and County agree to act immediately to mutually resolve any disputes which may arise with respect to this Agreement. All such disputes shall be subject to the provisions of this Paragraph 52 (such provisions shall be collectively referred to as the "Dispute Resolution Procedure"). Time is of the essence in the resolution of disputes.
- 52.2 Contractor and County agree that, the existence and details of a dispute notwithstanding, both parties shall continue without delay their performance hereunder.
- 52.3 Neither party shall delay or suspend its performance during the Dispute Resolution Procedure.
- 52.4 In the event of any dispute between the parties with respect to this Agreement, Contractor and County shall submit the matter to their respective Project Managers for the purpose of endeavoring to resolve such dispute.
- 52.5 In the event that the Project Managers are unable to resolve the dispute within a reasonable time not to exceed ten (10) days from the date of submission of the dispute to them, then the matter shall be immediately submitted to the parties' respective Project Directors for further consideration and discussion to attempt to resolve the dispute.
- 52.6 In the event that the Project Directors are unable to resolve the dispute within a reasonable time not to exceed ten (10) days from the date of submission of the dispute to them, then the matter shall be immediately submitted to Contractor's Project Executive and the Director. These persons shall have ten (10) days to attempt to resolve the dispute.
- 52.7 In the event that at these levels, there is not a resolution of the dispute acceptable to both parties, then each party may assert its other rights and remedies provided under this Agreement and/or its rights and remedies as provided by law.

- 52.8 All disputes utilizing this Dispute Resolution Procedure shall be documented in writing by each party and shall state the specifics of each alleged dispute and all actions taken. The parties shall act in good faith to resolve all disputes. At all three (3) levels described in this Paragraph 52, the efforts to resolve a dispute shall be undertaken by conference between the parties' respective representatives, either orally, by face to face meeting or by telephone, or in writing by exchange of correspondence.
- 52.9 Notwithstanding the foregoing, in the event of County's infringement of Contractor's intellectual property rights under the Agreement or violation by either party of the confidentiality obligations hereunder, the violated party shall have the right to seek injunctive relief against the other without waiting for the outcome of the Dispute Resolution Procedure.
- 52.10 Notwithstanding any other provision of this Agreement, County's right to seek injunctive relief to enforce the provisions of Paragraph 18 (Confidentiality and Security) shall not be subject to this Dispute Resolution Procedure. The preceding sentence is intended only as a clarification of County's rights and shall not be deemed to impair any claims that County may have against Contractor or County's rights to assert such claims after any such injunctive relief has been obtained.

53. ASSIGNMENT BY COUNTY

This Agreement may be assigned in whole or in part by County, without the further consent of Contractor, to a party which is not a competitor of Contractor and which agrees in writing to perform County's obligations under this Agreement.

54. NEW TECHNOLOGY

Contractor and County acknowledge the probability that the technology of the software and hardware which comprise the System will change and improve during the term of this Agreement. County desires the flexibility to incorporate into the System any new technologies as they may become available. Accordingly, Contractor's Project Manager shall, promptly upon discovery and on a continuing basis, apprise County's Project Director of all new technologies, methodologies and techniques which Contractor considers to be applicable to the System. Specifically, upon County's request, Contractor shall provide, in writing, a description of such new technologies, methodologies and techniques, indicating the advantages and disadvantages of incorporating same into the System, and provide an estimate of the impact such incorporation will have on the performance, scheduling and price of the System. County, at its sole discretion, may request that this Agreement be amended to incorporate the new technologies, methodologies and techniques into the System pursuant to the provisions of Paragraph 4 (Changes Notices and Amendments).

55. NON-DISCRIMINATION IN SERVICES

- 55.1 Contractor shall not discriminate in the provision of services hereunder because of race, color, religion, national origin, ancestry, sex, age, or physical or mental handicap, in accordance with all applicable requirements of Federal and State law. For the purpose of this Paragraph 55, discrimination in the provision of services may include, but is not limited to, the following: denying any person any service or benefit or the availability of the facility, providing any service or benefit to any person which is not equivalent or is not provided in an equivalent manner or at an equivalent time to that provided to others; subjecting any person to segregation or separate treatment in any manner related to the receipt of any service; restricting any person in any way in the enjoyment of any advantage or privilege

enjoyed by others receiving any service or benefit; and treating any person differently from others in determining admission, enrollment quota, eligibility, membership, or any other requirements or conditions which persons must meet in order to be provided any service or benefit.

- 55.2 Contractor shall ensure that recipients of services under this Agreement are provided services without regard to race, color, religion, national origin, ancestry, sex, age, or condition of physical or mental handicap.

56. UNLAWFUL SOLICITATION

Contractor shall inform all of its employees who provide services hereunder of the provisions of Article 9 of Chapter 4 of Division 3 (commencing with Section 6150) of California Business and Professions Code (i.e., State Bar Act provisions regarding unlawful solicitation as a runner or capper for attorneys) and shall take positive and affirmative steps in its performance hereunder to ensure that there is no violation of such provisions by its employees.

57. GOVERNING LAW, JURISDICTION AND VENUE

This Agreement shall be governed by, and construed in accordance with, the substantive and procedural laws of the State of California applicable to agreements made and to be performed within the State. Contractor agrees and consents to the exclusive jurisdiction of the courts of the State of California for all purposes regarding this Agreement and further agrees and consents that venue of any action brought hereunder shall be exclusively in the County of Los Angeles, California. For claims that are subject to exclusive Federal subject matter jurisdiction, Contractor agrees and consents to the exclusive jurisdiction of the Federal District Court of the Central District of California.

58. WAIVER

No breach of any provision hereof can be waived unless in writing. No waiver by County or Contractor of any breach of any provision of this Agreement shall constitute a waiver of any other breach or of such provision. Failure of County or Contractor to enforce at any time, or from time to time, any provision of this Agreement shall not be construed as a waiver thereof. The rights and remedies set forth in this Agreement shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Agreement.

59. AUTHORIZATION WARRANTY

Contractor and County represent and warrant that the person executing this Agreement or any Amendment thereto pursuant to Paragraph 4 (Changes Notices and Amendments) on its behalf is an authorized agent who has actual authority to bind it to each and every term, condition and obligation of this Agreement, and that all requirements of Contractor and County have been fulfilled to provide such actual authority.

60. VALIDITY AND SEVERABILITY

60.1 VALIDITY

The invalidity of any provision of this Agreement shall not render the other provisions hereof invalid, unenforceable or illegal, unless the essential purposes of this Agreement shall be materially impaired thereby.

60.2 **SEVERABILITY**

In the event that any provision herein contained is held to be invalid, void or illegal by any court of competent jurisdiction, the same shall be deemed severable from the remainder of this Agreement, if practicable, and shall in no way affect, impair or invalidate any other provision contained herein. If any such provision shall be deemed invalid in its scope or breadth, such provision shall be deemed valid to the extent of the scope or breadth permitted by law. If any provision of this Agreement is adjudged void or invalid for any reason whatsoever, but would be valid if part of the wording thereof were deleted or changed, then such provision shall apply with such modifications as may be necessary to make it valid and effective.

61. **NOTICES**

61.1 All notices or demands required or permitted to be given or made under this Agreement, unless otherwise specified, shall be in writing and shall be addressed to the parties at the following addresses and delivered: (i) by hand with signed receipt; (ii) by first class registered or certified mail, postage prepaid; or (iii) by facsimile or electronic mail transmission followed within twenty-four (24) hours by a confirmation copy mailed by first-class registered or certified mail, postage prepaid. Notices shall be deemed given at the time of signed receipt in the case of hand delivery, three (3) days after deposit in the United States mail as set forth above, or on the date of facsimile or electronic mail transmission if followed by timely confirmation mailing. Addresses may be changed by either party by giving ten (10) days prior written notice thereof to the other party.

61.2 Director shall have the authority to issue all notices or demands which are required or permitted to be issued by County under this Agreement.

61.3 To County, notices shall be sent to the attention of County's Project Manager and County's Project Director at the respective addresses specified in Section 1 (County Key Personnel) of Exhibit E (Administration of Agreement).

To Contractor, notices shall be sent to the attention of Contractor's Project Manager at the address specified in Section 2 (Contractor Key Personnel) of Exhibit E (Administration of Agreement), with a copy to Contractor's Project Executive.

61.4 Each party may change the names of the people designated to receive notices pursuant to this Paragraph 61 by giving written notice of the change to the other party, subject to County's right of approval in accordance with Paragraph 3.3 (Approval of Contractor's Staff).

62. **ARM'S LENGTH NEGOTIATIONS**

This Agreement is the product of arm's length negotiations between Contractor and County, with each party having had the opportunity to receive advice from and representation by independent counsel of its own choosing. As such, the parties agree that this Agreement is to be interpreted fairly as between them and is not to be strictly construed against either as the drafter or otherwise.

63. **NON-EXCLUSIVITY**

Nothing herein is intended nor shall be construed as creating any exclusive arrangement with Contractor. This Agreement shall not restrict County from acquiring similar, equal or like goods and/or services from other entities or sources.

64. CAPTIONS AND PARAGRAPH HEADINGS

Captions and paragraph headings used in this Agreement are for convenience only, are not a part of this Agreement, and shall not be used in construing this Agreement. If there is a conflict when referencing a Paragraph in this Agreement, between the Paragraph heading title and its number, the Paragraph heading title shall control.

65. FORCE MAJEURE

Neither party shall be liable for failure to perform under this Agreement, if its failure to perform arises out of, and only, fires, floods, epidemics, quarantine restrictions, other natural occurrences, strikes, freight embargoes or acts of terrorism, but in every such case the failure to perform must be totally beyond the control and without any fault or negligence of the non-performing party.

66. FORMS AND PROCEDURES

All existing forms and procedures used by Contractor in implementation of the provisions of this Agreement are deemed "approved" by County for purposes of this Paragraph 66. Any new forms and procedures which materially affect Contractor's performance of this Agreement shall be subject to review and approval by County prior to use by Contractor.

67. DAMAGE TO COUNTY FACILITIES, BUILDINGS AND GROUNDS

67.1 Contractor shall repair, or cause to be repaired, at its own cost, any and all damage to County facilities, buildings, or grounds caused by Contractor or employees or agents of Contractor. Such repairs shall be made immediately after Contractor has become aware of such damage, but in no event later than thirty (30) days after the occurrence.

67.2 If Contractor fails to make timely repairs, County may make any necessary repairs. All costs incurred by County, as determined by County, for such repairs shall be repaid by Contractor by cash payment upon demand or, without limitation of all County's other rights and remedies provided by law or under this Agreement, County may deduct such costs from any amounts due Contractor from County under this Agreement.

68. MINIMUM AGE, LANGUAGE SKILLS AND LEGAL STATUS OF CONTRACTOR PERSONNEL AT FACILITY

Contractor cannot assign employees under the age of eighteen (18) to perform Work under this Agreement. All of Contractor's employees working at County facilities must be able to communicate in English. Contractor's employees must be United State citizens or legally present and permitted to work in the United States.

69. NOTICE OF DELAYS

Exception as otherwise provided herein, when either party has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this Agreement, that party shall, within five (5) Business Days, give notice thereof, including all relevant information with respect thereto, to the other party.

70. RE-SOLICITATION OF BIDS AND PROPOSALS

70.1 Contractor acknowledges that, prior to the expiration or earlier termination of this Agreement, County, in its sole discretion, may exercise its right to invite bids or request proposals for the continued provision of the goods and services delivered or contemplated

under this Agreement. County shall make the determination to re-solicit bids or request proposals in accordance with applicable County policies.

- 70.2 Contractor acknowledges that County, in its sole discretion, may enter into an agreement for the future provision of goods and services, based upon the bids or proposals received, with a provider or providers other than Contractor. Further, Contractor acknowledges that it obtains no greater right to be selected through any future invitation for bids or request for proposals by virtue of its present status as Contractor.

71. NO PAYMENT FOR SERVICES PROVIDED FOLLOWING EXPIRATION OR TERMINATION OF AGREEMENT

Contractor shall have no claim against County for payment of any money or reimbursement, of any kind whatsoever, for any services provided by Contractor after the expiration or other termination of this Agreement. Should Contractor receive any such payment, it shall immediately notify County and shall immediately repay all such funds to County. Payment by County for services rendered after expiration/termination of this Agreement shall not constitute a waiver of County's right to recover such payment from Contractor. The provisions of this Paragraph 71 shall survive the expiration or other termination of this Agreement.

72. ACCESS TO COUNTY FACILITIES

Contractor, its employees and agents, may be granted access to County facilities, subject to Contractor's prior notification to County's Project Manager, for the purpose of executing Contractor's obligations hereunder. Access to County facilities shall be restricted to normal business hours, 8:00 a.m. until 5:00 p.m., Pacific Time, Monday through Friday, County observed holidays excepted. Access to County facilities outside of normal business hours must be approved in writing in advance by County's Project Manager, which approval will not be unreasonably withheld. Contractor shall have no tenancy, or any other property or other rights, in County facilities. While present at County facilities, Contractor's personnel shall be accompanied by County personnel at all times, unless this requirement is waived in writing prior to such event by County's Project Manager.

73. COUNTY FACILITY OFFICE SPACE

In order for Contractor to perform Services hereunder and only for the performance of such Services, County may elect, subject to County's standard administrative and security requirements, to provide Contractor with office space and equipment, as determined at the discretion of the applicable County's Project Manager at County facilities, on a non-exclusive use basis. County shall also provide Contractor with reasonable telephone service in such office space for use only for purposes of this Agreement. County disclaims any and all responsibility for the loss, theft or damage of any property or material left at such County office space by Contractor.

74. PHYSICAL ALTERATIONS

Contractor shall not in any way physically alter or improve any County facility without the prior written approval of the Director, County's Project Director and the Director of County's Internal Services Department, in their discretion.

75. STAFF PERFORMANCE WHILE UNDER THE INFLUENCE

Contractor shall use reasonable efforts to ensure that no employee of Contractor shall perform services hereunder while under the influence of any alcoholic beverage, medication, narcotic or other substance which might impair his or her physical or mental performance.

76. RECYCLED PAPER

Consistent with the County's Board of Supervisors' policy to reduce the amount of solid waste deposited at the County landfills, Contractor agrees to use recycled-content paper to the maximum extent possible in this project.

77. TIME OFF FOR VOTING

Contractor shall notify its employees, and shall require each subcontractor to notify and provide to its employees, information regarding the time off for voting law (Elections Code Section 14000). Not less than ten (10) days before every statewide election, Contractor and subcontractors shall keep posted conspicuously at the place of work, if practicable, or elsewhere where it can be seen as employees come or go to their place of work, a notice setting forth the provisions of such Section 14000.

78. SURVIVAL

In addition to any provisions in this Agreement which specifically state that they shall survive the termination or expiration of the Agreement, the provisions in the following Paragraphs shall also survive the expiration or termination of this Agreement for any reason:

- 2.4 Approval of Work
- 9.5 County's Right to Withhold Payment
- 10 System Ownership and License
- 12 Warranties and Correction of Deficiencies
- 13 Indemnification
- 14 Insurance
- 15 Intellectual Property Warranty and Indemnification
- 16 Proprietary Considerations
- 17 Disclosure of Information
- 18 Confidentiality and Security
- 24 Effect of Termination
- 29 Records and Audits
- 32 Compliance with Applicable Laws
- 33 Fair Labor Standards

36	Employment Eligibility Verification
40	Federal Access to Records
42	No Third Party Beneficiaries
51	County Audit Settlements
57	Governing Law, Jurisdiction and Venue
60	Validity and Severability

/

/

/

IN WITNESS WHEREOF, County and Contractor by their duly authorized signatures have caused this Agreement to be effective on the day, month and year first above written.

COUNTY OF LOS ANGELES:
LOS ANGELES COUNTY SHERIFF'S DEPARTMENT

By _____
JIM McDONNELL
SHERIFF

CONTRACTOR:
NEC CORPORATION OF AMERICA

By _____
Signature
Raffie Beroukhim
Print Name
Vice President, Biometrics Solutions Division
Title

APPROVED AS TO FORM:
MARK J. SALADINO
County Counsel

By _____
VICTORIA MANSOURIAN
Principal Deputy County Counsel

**AGREEMENT
FOR
MBIS SOLUTION**



EXHIBIT A
STATEMENT OF WORK

DECEMBER 2014

TABLE OF CONTENTS

SECTION 1	SCOPE OF WORK	1
Section 1.1	Overview	1
Section 1.2	Project Objectives	2
Section 1.2.1	Scope of work.....	2
Section 1.2.2	Project Management	3
Section 1.3	Document References	3
Section 1.3.1	Compliance Documents	3
Section 1.3.2	Specifications, Standards and Guides	3
Section 1.4	Definitions	4
SECTION 2	SYSTEM IMPLEMENTATION TASKS AND DELIVERABLES.....	6
TASK 1 – PROJECT ADMINISTRATION		7
Subtask 1.1 – Develop Project Plans.....		8
Deliverable 1.1 – Project Plans		8
Subtask 1.2 – Prepare Status Reports and Conduct Conferences		10
Deliverable 1.2 – Complete Status Reports And Conferences.....		14
TASK 2 – SYSTEM SETUP.....		14
Subtask 2.1 – Provide Data and Property Management		15
Deliverable 2.1 – Data And Property Management		20
Subtask 2.2 – Implement System Security		20
Deliverable 2.2 – Secured System Environment		20
TASK 3 – SYSTEM IMPLEMENTATION		20
Subtask 3.1 – Conduct System Requirements Review		21
Deliverable 3.1 – System Requirements Specifications		26
Subtask 3.2 – Perform System Design and Development.....		26
Deliverable 3.2 – System Design and Development		31
TASK 4 – CONDUCT ACCEPTANCE TESTS		32
Subtask 4.1 – Conduct Factory Acceptance Test.....		34
Deliverable 4.1 – Factory Acceptance Testing		36
Subtask 4.2 – Conduct System Acceptance Test.....		37
Deliverable 4.2 – System Acceptance Testing		39
Subtask 4.3 – Conduct User Acceptance Test.....		40
Deliverable 4.3 – User Acceptance Testing.....		41
TASK 5 – SYSTEM MIGRATION		41
Subtask 5.1 – Install Sites.....		55
Deliverable 5.1 – Install Sites.....		55
Subtask 5.2 – Convert And Load Data		56
Subtask 5.2.1 – Convert Existing Data		56
Deliverable 5.2.1 – Converted Existing Data		57

Subtask 5.2.2 – Load Data	57
Deliverable 5.2.2 – Loaded Data	58
Subtask 5.3 – Conduct Migration Planning.....	58
Deliverable 5.3 – Migration Plan	59
TASK 6 – CONDUCT SYSTEM TRAINING	59
Deliverable 6 – System Training and Materials	61
TASK 7 – CONDUCT REMAINING MIGRATION TASKS	62
Subtask 7.1 – Manage System Configuration	62
Deliverable 7.1 – System Configuration Plan	68
Subtask 7.2 – Continuity of Operations Planning	68
Deliverable 7.2 – Coop Plan	73
Subtask 7.3 – Conduct Final Acceptance Test.....	73
Deliverable 7.3 – Final Acceptance	74

STATEMENT OF WORK

SECTION 1 SCOPE OF WORK

This Exhibit A sets forth the Statement of Work ("SOW") for the implementation and the operation of the Multimodal Biometric Identification System ("MBIS") for the County of Los Angeles ("County") during the term of the Agreement. The SOW consists of the of tasks, subtasks, deliverables, goods, services and other Work that Contractor shall be required to provide under the Agreement. In addition to the other requirements of this SOW, Contractor shall provide the Deliverables identified in Attachment 2 – Project Deliverables.

Unless agreed to by County and with proper CJIS authorization, all Work performed under the Agreement shall be performed within the territory of the United States and shall be performed by United States citizens or Lawful Permanent Residents of the United States. No County data (including without limitation biometric data, identity history data, biographic data, property data and case/incident history data, as defined in the CJIS Security Policy under Section 1.3.2 – Specifications, Standards and Guides above or information) shall be communicated to anyone who is not a United States citizen or Lawful Permanent Resident of the United States. County data shall not be stored, accessed from or transmitted to outside of the United States without County's written permission provided in advance. County shall have the right, from time to time, to designate certain subsets of County data as being subject to additional storage, access or transmission restrictions at its sole discretion.

SECTION 1.1 OVERVIEW

The County's Sheriff's Department ("LASD") has selected the Contractor via an open and competitive solicitation an MBIS solution ("Solution"), to ensure that County is getting the best value for the required Work, to replace its Existing System, LACRIS Automated Finger Print Identification System ("LAFIS").

Contractor's response to the RFP includes, but is not limited to, System hosting, software licensing and implementation, project management, training, customizations, data migration, ongoing maintenance, support and reporting services, all based on a Commercial Off-The-Shelf ("COTS") software.

Contractor will also be required to provide initial training, data extraction, optional customizations, data migration and hosting services as part of the tasks outlined in this Statement of Work. The proposed Solution will meet the minimum requirements of this project and is a best match to provide County's requirements.

This will be a Contractor managed Solution, which shall include all hardware and software, including maintenance releases. Contractor shall supply all levels of technical support set forth in the Contractor developed Service Level Plan, which shall meet all requirements under Section 3 – System Operation of this Exhibit A and Exhibit D (Service Level Requirements).

The Scope of Work to be provided by Contractor under the Agreement consists of two phases: System Implementation and System Operation.

This Statement of Work will be the basis for a Project Management Plan and a Project Schedule. All Work under the Agreement shall be performed at the rates and fees set forth in a Pricing Schedule based on the submitted cost proposal and is part of this Agreement.

Contractor shall perform, complete and deliver all Work, however denoted, as set forth in this Statement of Work. Also defined herein are those Tasks and Subtasks that involve participation of both Contractor and County. Unless otherwise specified as an obligation of County, Contractor shall perform all Tasks and Subtasks and provide all Deliverables as defined herein. A Deliverable shall only be deemed complete upon County's approval and Acceptance, irrespective of the number of attempts it takes Contractor to provide a successful Deliverable.

Contractor shall be responsible for furnishing all personnel, facilities, equipment, material, supplies, and support and management services and shall perform all functions necessary to satisfy the requirements of this SOW and the System Requirements set forth in Attachment A.1 – System Requirements. All of System Requirements, whether specifically referenced or not in this SOW, shall apply to Contractor's deliverables under the Agreement.

The following Attachments setting forth the Statement of Work requirements and specifications are attached to and form a part of this Statement of Work:

- **ATTACHMENT A.1 – SYSTEM REQUIREMENTS**
- **ATTACHMENT A.2 – PROJECT DELIVERABLES**
- **ATTACHMENT A.3 – PERFORMANCE REQUIREMENTS**
- **ATTACHMENT A.4 – SYSTEM CONFIGURATION**
- **ATTACHMENT A.5 – EXISTING SYSTEM REPORT**

SECTION 1.2 PROJECT OBJECTIVES

SECTION 1.2.1 SCOPE OF WORK

Contractor shall provide, implement and support for the County a biometric technology Solution (MBIS) that will:

- Provide a biometric and web services standards based open architecture that
 - Enables implementation of state-of-the-art AFIS (e.g. 10 print, palm print, latent) applications and work flows including integration with the current Live-Scan fingerprint and mug shot systems
 - Provides for incremental enhancement/addition/replacement of applications and work flows for fingerprinting and facial data capture, iris, voice, scar, marks and tattoos, facial recognition and DNA biometric toolsets
 - Allows selection of best-of-breed applications from different vendors; provides for use of non-proprietary hardware, database software and open-standards application software interfaces
 - Stores integrated subject biometric data (captured via the various biometric toolsets) that enables online inquiries and reporting based on integrated subject biometric data
- Be sized for planned growth
- Utilize ANSI/NIST/FBI record constructs
- Conform to national and international biometric standards

-
- Use Commercial Off-The-Shelf (COTS) hardware and software
 - Provide configurable administrative controls
 - Manage orchestration and transaction integrity of all sub-components of the MBIS Solution
 - Manage and control biometric data using subject biometric identifiers as keys
 - Provide efficient and cost-effective storage and retrieval
 - Detect and notify when systems, applications, equipment or networks are interrupted or when there is a loss of power
 - Provide an operational County-approved Disaster Recovery Site
 - Provide for migration of fingerprints and mug shots from already existing County systems.

SECTION 1.2.2 PROJECT MANAGEMENT

Contractor shall provide full project management, planning, monitoring, supervision, tracking and control of all project activities during the term of the Agreement. Contractor shall employ project management industry standards and practices in the performance of all Work.

SECTION 1.3 DOCUMENT REFERENCES

SECTION 1.3.1 COMPLIANCE DOCUMENTS

Referenced or applicable documents cited within the Agreement, including this SOW, shall be considered compliance documents for the purpose of the Agreement. County recognizes that some of the compliance documents and their associated data items listed below may change. Throughout the term of the Agreement, Contractor or County may propose compliance with newer documents and their associated data items that replace or supersede those identified in this list. To substitute newer documents and their associated data items, Contractor shall perform all of the following, in the order as listed:

1. Identify existing standards and data items to be replaced;
2. Identify new documents and associated data items proposed for use;
3. Provide a rationale for using the new items including cost, schedule, performance and supportability impact; and
4. Obtain County approval.

SECTION 1.3.2 SPECIFICATIONS, STANDARDS AND GUIDES

The following documents identified in this section below constitute the specifications, standards and guides serving as the core reference materials for the MBIS:

- System Requirements, including those identified in Attachment A.1 – System Requirements
- American National Standards Institute/National Institute of Standards and Technology (ANSI/ NIST) ANSI/NIST-ITL 1-2011 Data Format for the Interchange of Biometric and Forensic Information, dated November 2011
- Electronic Biometric Transmission Specification (EBTS), NGI-DOC-01078-10.0.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.

SECTION 1.4 DEFINITIONS

The capitalized terms listed below that are used throughout this Exhibit A shall have the definitions given to such terms in this section. All other capitalized terms used in this Exhibit A without definitions shall have the meanings given to such terms in the Base Agreement.

1. "COOP Plan" shall have the meaning specified in Subtask 7.2 – Continuity of Operations Planning.
2. "COOP Site" shall have the meaning specified in Task 3 – System Implementation.
3. "COTS" shall have the meaning specified in Section 1.1 – Overview.
4. "Critical Deficiency" shall mean a Deficiency of Priority Level 1, as further specified in Section 3.5.2 – Deficiency Priority Levels.
5. "Customer Support" shall have the meaning specified in Section 3.2.2 – Customer Support.
6. "Data Migration" shall mean and refer to the tasks, subtasks and deliverables provided by Contractor pursuant to Task 5 – System Migration.
7. "Disaster" shall mean a catastrophic event that results in significant or potentially significant Downtime or disruption of the Operational Environment and requires Contractor to invoke the Disaster Recovery Plan.
8. "Disaster Recovery" shall have the meaning specified in shall mean Contractor's obligations set forth in Section 3.7 – Continuity of Operations.
9. "Disaster Recovery Plan" shall have the same meaning as "COOP Plan".
10. "Downtime" shall mean the period of time when the Solution or any Solution component is unavailable, including Scheduled Downtime and Unscheduled Downtime.
11. "Existing System" shall have the meaning specified in Subtask 5.3 – Conduct Migration Planning.
12. "Factory Acceptance Test" shall have the meaning specified in Subtask 4.1 – Conduct Factory Acceptance Test.
13. "FAR" shall have the meaning specified in Subtask 7.3 – Conduct Final Acceptance Test.
14. "Final Acceptance" shall have the meaning specified in Deliverable 7.3 – Final Acceptance.
15. "Final Acceptance Test" shall have the meaning specified in Subtask 7.3 – Conduct Final Acceptance Test.
16. "Implementation Period" shall mean the period from the Effective Date of the Agreement through the Solution's Final Acceptance by County.
17. "Integrated Master Schedule"; "IMS" shall have the meaning specified in Task 1 – Project Administration.
18. "LACRIS" shall mean the Los Angeles County Regional Identification System of the County's Sheriff.
19. "LAFIS" shall have the meaning specified in Section 1.1 – Overview.
20. "Low Deficiency" shall a Deficiency of Priority Level 4, as further specified in Section 3.5.2 – Deficiency Priority Levels.

21. "Maintenance Period" shall mean the period from Final Acceptance through the end of the term of the Agreement.
22. "Maintenance Services" shall mean any goods and/or services provided by Contractor under the Agreement for maintaining the Solution, including but not limited to Software Updates, Hardware Upgrades, enhancements, corrections and other updates to the Solution, interfaces, performance, data security, reports and regulatory compliance, as further specified in Section 3.4 – Maintenance Services and this Statement of Work.
23. "Major Deficiency" shall mean a Deficiency of Priority Level 1 or Priority Level 2, as further specified in Section 3.5.3 – Problem Resolution and Protocols.
24. "Migration Plan" shall mean the plan for Data Migration provided by Contractor pursuant to Subtask 5.3 – Conduct Migration Planning.
25. "Moderate Deficiency" shall mean a Deficiency of Priority Level 3, as further specified in Section 3.5.2 – Deficiency Priority Levels.
26. "Operational Environment" shall mean the System Environment set up by Contractor as part of System Implementation for Operational Use of the System under the Statement of Work.
27. "Operational Use" shall mean actual use of the System in the Operational Environment for the performance of County's operations upon Final Acceptance.
28. "Phase 1" shall have the same meaning as "System Implementation Phase".
29. "Phase 2" shall have the same meaning as "System Operation Phase".
30. "Primary Site" shall mean County's primary Operational Use site for the System.
31. "Priority Level" shall mean the applicable Deficiency severity level for correcting Deficiencies, as further specified in Section 3.5.1 – Identification of Deficiencies.
32. "Project Management Plan"; "PMP" shall have the meaning specified in Subtask 1.1 – Develop Project Plans.
33. "Project Plan" shall have the meaning specified in Task 1 – Project Administration.
34. "Remote Site" shall mean any one of locations where either tenprint or latent workstations are installed for the use of the System.
35. "Response Time" shall mean the time elapsed from the end of ingest through the final response, to the return of a response from the MBIS to the submitting device with no error TOTs in the mix, as further specified in Section 3.4.5 – Response Time Monitoring.
36. "Scheduled Downtime" shall mean the Solution cannot be accessed due to System scheduled maintenance, including but not limited to preventive maintenance, updates, upgrades, scheduled reboots and restarts, as further specified in Section 3.4.4 – Scheduled Downtime and Preventive Maintenance.
37. "Service Availability" shall have the meaning specified in Section 3.2.3 – Service Level Performance.
38. "Service Level Plan" shall have the meaning specified in Section 3 – System Operation.
39. "Service Level(s)"; "Service Level Requirements" shall mean the requirements of Contractor's service levels during System Operation specified in the Agreement, including Section 3 – System Operation, Attachment A.3 – Performance Requirements to this Exhibit A and Exhibit D (Service Level Requirements).

-
40. "Severe Deficiency" shall mean a Deficiency of Priority Level 2, as further specified in Section 3.5.2 – Deficiency Priority Levels.
 41. "Support Hours" shall have the meaning specified in Section 3.2.2 – Customer Support.
 42. "Support Services" shall mean any goods and/or services provided by Contractor under the Agreement in support of the Solution, including but not limited to, updates, corrections, enhancements, customer support, interfaces, performance, data security, reports and applicable regulatory compliance, as further specified in Section 3.2.2 – Customer Support and this Statement of Work.
 43. "System Acceptance Test" shall have the meaning specified in Subtask 4.2 – Conduct System Acceptance Test.
 44. "System Implementation" shall mean Contractor's responsibilities and other Work relating to the implementation of the System, as further specified in Section 2 – System Implementation Tasks and Deliverables.
 45. "System Implementation Phase" shall mean the System Implementation phase of the Statement of Work.
 46. "System Operation" shall mean Contractor's responsibilities and other Work relating to the Operational Use of the System, as further specified in Section 3 – System Operation.
 47. "System Operation Phase" shall mean the System Operation phase of the Statement of Work.
 48. "System Performance" shall mean the performance of the System with respect to Response Time, Service Availability and Disaster Recovery.
 49. "System Performance Deficiency" shall mean the System not meeting any one of the System Performance Requirements set forth in this Statement of Work, including Attachment A.3 – Performance Requirements.
 50. "System Performance Requirements" shall mean the requirements for System Performance, including Attachment A.3 – Performance Requirements.
 51. "TOT" shall mean type of transaction.
 52. "Training Plan" shall have the meaning specified in Deliverable 6 – System Training and Materials.
 53. "UAT Plan" shall have the meaning specified in Subtask 4.3 – Conduct User Acceptance Test.
 54. "Unscheduled Downtime" shall have the meaning specified in Section 4.1 – Service Credits.
 55. "User Acceptance Test"; UAT shall have the meaning specified in Subtask 4.3 – Conduct User Acceptance Test.

SECTION 2 SYSTEM IMPLEMENTATION TASKS AND DELIVERABLES

This Section of the SOW, together with Attachment A.1 – System Requirements, Attachment A.2 – Project Deliverables and Attachment A.3 – Performance Requirements, provides a detailed description of the scope of Work to be performed by Contractor throughout the System implementation phase (Section 2 – System Implementation Tasks and Deliverables) of the Agreement, including MBIS development, implementation and testing.

Contractor will comply with the program organization requirements of Task 1 – Project Administration outlined below.

Contractor Program Organization shall use a proven PMBOK-based methodology that provides a quality implementation. The Program Organization is created to ensure that the project meets its objectives and delivers the projected benefits on schedule. Contractor shall identify the tools and procedures to manage project baselines as appropriate to the requirements of the project.

Contractor believes that achieving client satisfaction, and successful project performance is interrelated and involves sound Project and Program Management practices throughout the entire project life cycle.

Key responsibilities of Contractor's Project Manager shall include:

- Understanding and documenting the County's stakeholder goals and strategic objectives and ensuring that project scope and requirements are aligned with these objectives,
- Clear and constant communications from the Project Management Team,
- Detailed and measurable acceptance criteria for project deliverables,
- Engaging County stakeholders early in the design and development process to confirm that expectations are being met.

Specifically, this involves activities such as:

- Working with the County to understand and document clear and measurable business requirements and project objectives. Project objectives are documented in the Project Charter, whereby Contractor's Project Manager will ensure County's Project Director's approval of the Project Charter and requirements.
- Managing change through a formal configuration and change management process. This ensures the County approves all changes and helps to keep expectations in line.
- Periodic assessment of performance to ensure that commitments are being met. If there is a variance from the prior commitments, Contractor's Project Manager addresses these issues to ensure that the project realigns within expectations.
- Performing a Factory Acceptance Test with County resources prior to shipping the Solution to ensure that expectations are being met and any concerns are addressed as quickly as possible.
- Ongoing proactive communication with project stakeholders, including conducting recurring progress meetings and distributing minutes and progress reports afterwards. Contractor's Project Manager will keep the project team well informed throughout the project on progress, issues, and risks. Consistency with information distribution and performance reporting is a key role of Contractor's Project Manager.

Through these and other related activities, the Contractor Project Management Team will work to not only achieve but to exceed expectations.

TASK 1 – PROJECT ADMINISTRATION

The provisions of this Task 1 – Project Administration describe the requirements for the project management functions to be performed by Contractor during the System Implementation phase of the Agreement. Contractor shall document management organization, roles and

responsibilities, resources, processes and other pertinent management information in project plans ("Project Plan(s)"), including a Project Management Plan [DEL-01] and Integrated Master Schedule ("IMS") [DEL-03] and maintain such plans current as necessary throughout the System Implementation phase.

SUBTASK 1.1 – DEVELOP PROJECT PLANS

Contractor shall review the System Requirements with County's Project Manager. Based upon that review, Contractor shall have the primary responsibility of preparing a project plan document ("Project Management Plan") and submitting it for written approval to County's Project Manager. County shall work closely with Contractor during the preparation of the Project Management Plan. County shall have the final discretion in requiring an order of tasks and deliverables and/or a dependency of paid and unpaid tasks and deliverables to other paid or unpaid tasks and deliverables.

Additionally, Contractor shall develop an Integrated Master Schedule (IMS) [DEL-03] and keep it current throughout the System Implementation phase of the Agreement. The IMS shall be resource loaded and shall include, at a minimum, all activities required under this Statement of Work, including all management and technical reviews. The IMS shall identify activities by applicable Site (Primary Site, COOP Site and Remote Sites). The IMS shall identify any schedule margin/reserve. The IMS shall provide sufficient detail to demonstrate confidence that the schedule is complete and realistic. The IMS shall identify due dates associated with any County-furnished items (e.g., information, data, facilities access) and due dates associated with all Contractor Deliverable items.

Contractor will comply with the program organization requirements to develop and maintain a Project Management Plan, which includes all items described in this section.

The Project Management Plan (DEL-01) is a formal, approved document for managing and ensuring the successful implementation of the MBIS solution. The PMP defines the project attributes and Project Management processes and plans shown in Deliverable 1.1 – Project Plans below.

APPLICABLE STANDARDS

Project Management Institute – Project Management Body of Knowledge (PMBOK), fifth edition.

DELIVERABLE 1.1 – PROJECT PLANS

Contractor shall provide for County's approval the Project Management Plan developed in County-specified version of Microsoft Project (currently 2010), which shall, at a minimum, include the following:

1. All Work described in this Statement of Work and elsewhere in the Agreement including:
 - a. All Deliverables, including those referenced in the Pricing Schedule,
 - b. All Tasks, Subtasks, Deliverables and other Work,
 - c. Associated dependencies, if any, among Tasks, Subtasks, Deliverables and other Work,
 - d. Resources assigned to each Task, Subtask, Deliverable and other Work,
 - e. Start date and date of completion for each Task, Subtask, Deliverable and other Work,

-
- f. Proposed County review period for each Deliverable,
 - g. Proposed Milestones, and
 - h. Other information reasonably required by County;
2. Identification of all Contractor Key Personnel and Contractor Key Staff;
 3. A Deficiency management plan, documenting the approach to Deficiency management, including methodology, recommended tool(s) and escalation process;
 4. Approach to project communications;
 5. A risk management plan, documenting the approach to risk analysis (e.g., the evaluation of risks and risk interactions to assess the range of possible project outcomes), risk mitigation (e.g., the identification of ways to minimize or eliminate project risks), risk tracking/control (e.g., a method to ensure that all steps of the risk management process are being followed and, risks are being mitigated effectively) and clearly establishing a process for problem escalation, to be updated, as needed, throughout the term of the Agreement;
 6. Initial identification of risks that may impact the timely delivery of the Solution;
 7. Project staffing and resource management plan;
 8. Configuration and change management plan. Changes, in this context, refer to changing the functionality of, or adding additional functionality (e.g., changes to the project scope) to, any Solution component. The approach shall ensure that the impact and rationale for each change are analyzed and coordinated prior to being approved; and
 9. Deliverable Acceptance Criteria which shall be based on the terms of the Agreement, including the Statement of Work and the actual tasks being completed, and shall include all documentation, whether stated in the SOW or not, that is consistent with good analytical practices, as determined by County.

Contractor shall prepare and provide to County a finalized Project Management Plan pursuant to Subtask 1.1 – Develop Project Plans. The Project Plan may be modified only if such modification has been approved in advance in writing by County’s Project Manager. The Project Management Plan shall be the basis for the Project Schedule, which shall be updated upon finalization of the Project Management Plan and shall be attached to the Agreement as Exhibit C (Project Schedule).

Contractor shall also develop an IMS, which shall include the activities required under this Statement of Work, as provided in Subtask 1.1 – Develop Project Plans.

The Deliverables required to be provided by Contractor under this Deliverable 1.1 – Project Plans shall include:

- **DEL-01:** Project Management Plan
- **DEL-03:** Integrated Master Schedule
- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes

Table 1: Management and Technical Reporting and Reviews

REVIEW	LOCATION
Project Kickoff Meeting	County Facility
System Requirements Review	County Facility
System Design Review	County Facility
Product Test Readiness Review	Contractor's Facility
Pre-Ship Review	Contractor's Facility
System Test Readiness Review	County Facility
Operational Readiness Review	County Facility
Final Acceptance Review	County Facility
Project Management Reviews	County Facility

SUBTASK 1.2 – PREPARE STATUS REPORTS AND CONDUCT CONFERENCES

Contractor shall provide ongoing project administration, which shall include, but not be limited to, the following:

1. Monthly written Project Plan update reports;
2. Weekly status update conference;
3. Attending meetings with County Executives and Management as needed; and
4. Updates to the Project Management Plan and the Project Schedule.

Contractor's Project Manager shall provide full project management and control of project activities. Contractor's Project Manager shall present to County's Project Manager written status reports documenting project progress, plans and outstanding issues. Contractor's Project Manager shall meet with or conduct a status update conference with County's Project Manager on a weekly basis, or as otherwise agreed to by County and Contractor, to review project status reports and any related matters. All variances shall be presented to County for approval at the status meetings. The first report shall be presented to County's Project Manager one (1) week following the Effective Date in a format approved by County. This Subtask 1.2 – Prepare Status Reports and Conduct Conferences shall include, but not be limited to:

1. Project planning and direction;
2. Contractor staffing and personnel matters, including management of Contractor technical staff;
3. Evaluation of results and status reporting;
4. Incorporation of County's System Requirements, including, but not limited to, all business, functional and technical requirements;
5. Incorporation of required software modification, if any; and
6. Management and tracking of all issues and their resolution.

Contractor's Project Manager and County's Project Manager shall report project status on a regular basis and shall participate in monthly status meetings. The project and reporting system shall include, but not be limited to, the following components:

1. Kick off meeting;
2. Updated Project Plan; and
3. Status reports and meetings or teleconferences.

The project status reports prepared by Contractor's Project Manager pursuant to this Subtask 1.2 – Prepare Status Reports and Conduct Conferences shall be used as the mechanism for Contractor to report any project risks or problems identified as part of the implementation process.

Contractor will comply with reporting and reviews set forth in Subtask 1.2 – Prepare Status Reports and Conduct Conferences, which includes proposed activities, deliverables, descriptions of deliverable content, and media.

The Communications Plan section of the Project Management Plan (**DEL-01**) details the reports, meetings, and deliverables that will be supplied during the implementation of the MBIS project. It includes the sections on recipient, format, timing, and responses required.

APPROACH

The Contractor Project team will assume full project management, monitoring and control of project activities. This involves directing, managing, monitoring and controlling activities, including:

- Project planning and direction: defining, preparing and integrating all project planning documentation, and leading and performing the work defined in the plans, management and tracking of all issues and their resolution, and implementing any approved changes to the project's objectives.
- Managing Contractor staging and personnel matters, including management of Contractor technical staff.
- Evaluating results and status reporting: tracking, reviewing and reporting project progress against the performance objectives defined in the PMP (**DEL-01**).

In support of these activities the Contractor Project Management Team will report status to, and participate in a series of meetings with the County. This includes, but is not limited to the following:

- Project Kickoff Meeting
- Monthly Status Meetings and monthly written Status Reports
- Weekly status update conferences
- Participation in County Executive and management meetings, as appropriate
- Documentation updates, including the PMP (**DEL-01**) and IMS (**DEL-03**), as appropriate
- Formalized Project Reviews that serve as approval or gating steps in the project life cycle

Project Kickoff Meeting

Within 10 working days after contract award, the Contractor Project Director, Contractor Project Manager, and key project personnel will meet with the County's project team at their facility for a project kickoff meeting. The key areas for discussion are outlined in the following draft agenda.

Draft Project Kick-off Meeting Agenda

1. Introductions of key County and Contractor project personnel.
2. Discuss submitted Project Management Plan and reach agreement on any areas of concern or requiring clarification.
3. Discuss the status and planned mitigation for all identified risks and issues.
4. Discuss any ideas proposed by county or Contractor in the approach to managing the project or the deliverables.
5. Discussion on any issues or areas of concern to County or Contractor project team members.

Contractor will submit an agenda 5 days prior to this meeting outlining any specific topics Contractor would like to address in this meeting.

Monthly Status Meetings and Reporting

The Contractor Project Director, Contractor Project Manager, and key project team members, as determined by the planned agenda, will conduct a Project Management Review (PMR) meeting within 60 days of contract award, and on a monthly basis thereafter, for the duration of the project. In advance of these meetings, Contractor will provide a monthly status report and any required presentation materials and supporting data, along with the agenda, to ensure topics are covered in an efficient and effective manner. A key objective of the Status Reports will be to formalize a mechanism for Contractor to report project risks or issues identified as part of the implementation process. Whenever possible, this meeting will be combined with other scheduled project meetings/reviews planned for the same time period. Meetings will include but are not limited to the following areas of discussion:

- Schedule status
- Proposed changes to the Integrated Master Schedule (DEL-03)
- Technical accomplishments
- Issues and risks
- Planned activities
- Quality Assurance findings and plans for corrective action
- County selected technical and programmatic topics

Weekly Status Update Conferences

On a weekly basis starting one week after contract award, the Contractor Project Manager along with the County's Project Manager will conduct Project Status Update Conferences. These conferences will be held for the duration of the project. The purpose

of the conference is to review project status reports and any related matters. Additionally, any variances will be presented to the County for approval at the status meetings.

All reviews as outlined in the RFP will be incorporated into the project at the appropriate points and are outlined in the Project Management Plan and Integrated Master Schedule along with any associated deliverables. Contractor will be able to effectively coordinate and implement all requested deliverables, activities, and description of deliverable content in a contemporary format of media such as DVD, Web URL, or other easily accessible and reliable method.

Project Reviews

A series of formal reviews will be conducted as part of the project life cycle. These include the Project Kickoff and Project Management Reviews described above. Other formal reviews are described in Table 2:

Table 2: Formal Reviews

REVIEW	PURPOSE
Systems Requirement Review (SRR)	Review the results of the System Requirements definition activity and recommend changes, as appropriate
System Design Review (SDR)	Review System Design deliverables, present evidence to demonstrate that the design satisfies the requirements of the County's SRS. Upon successful completion of the SDR, and written approval of the county, Contractor will begin development & procurement of System components.
Product Test Readiness Review (PTRR)	Review the state of the solution and its readiness for Factory Acceptance Test (FAT). Successful completion of the PTRR authorizes moving forward with the FAT.
Pre-ship Review (PSR)	Upon completion of the FAT, the PSR demonstrates success of FAT execution, and System readiness for delivery to LASD.
System Test Readiness Review (STRR)	Review the state of the solution and its readiness for System Acceptance Test (SAT). Successful completion of the STRR authorizes moving forward with the SAT.
Operational Readiness Review	Upon completion of the SAT, the ORR demonstrates success of SAT execution, and System readiness for User Acceptance Test (UAT).
Final Acceptance Review (FAR)	LASD will conduct a FAR to determine if CONTRACTOR has satisfied the requirements of the SOW and if the System can be accepted.

TOOLS AND METHODOLOGY

Communication Methods

Formal meetings as described in the section above, and informal communications, as appropriate within the project team. Also reference the supplemental Communications Management Plan in the Project Management Plan (DEL-01).

Information Distribution Tools

- **Agendas (DEL-07):** At a minimum, agendas will focus on information to present, issues to discuss, problems to solve, and decisions to make. Topics will have responsible owners and target discussion durations. Agendas will be submitted for review five days in advance of the meeting.
- **Presentation Materials (DEL-08):** Microsoft PowerPoint presentations and other materials, as appropriate. Presentation materials will be submitted for review five days in advance of the meeting; may be updated at the meeting and submitted as part of the meeting minutes.
- **Minutes (DEL-09):** Minutes will model the meeting agenda. Draft minutes will be delivered 2 days after a meeting, with the final version being submitted 5 days after receipt of County's comments.
- **Software:** The proposal responses lists the project management tools that Contractor will use throughout the project

DELIVERABLE 1.2 – COMPLETE STATUS REPORTS AND CONFERENCES

Contractor's Project Manager shall prepare and present to County's Project Manager written status reports documenting project progress, plans and outstanding issues in accordance with Subtask 1.2 – Prepare Status Reports and Conduct Conferences. Contractor's Project Manager shall meet with or conduct a status update conference with County's Project Manager, as agreed to by County and Contractor, to review project status reports and any related matters. All variances shall be presented for approval by County at the status conferences. The first report shall be presented to County's Project Manager one (1) week following the Effective Date in a format approved by County.

Contractor will provide the following deliverables:

- **DEL-01:** Project Management Plan
- **DEL-03:** Integrated Master Schedule
- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes

TASK 2 – SYSTEM SETUP

The Subtasks below in this Task 2 – System Setup provide for the setup and security of the future MBIS environment.

SUBTASK 2.1 – PROVIDE DATA AND PROPERTY MANAGEMENT

Contractor shall develop, document and implement comprehensive procedures for the management of data, documentation and County property (equipment, hardware and software that belongs to County). Data management shall encompass all data and documentation produced by Contractor under the Agreement, procured by Contractor under the Agreement and received from County for use on the Agreement.

Contractor will comply with the data and property management requirements of Subtask 2.1 – Provide Data and Property Management, including proposed activities, deliverables, and descriptions of deliverable content, delivery media, and County property (equipment, hardware, and software).

Contractor will develop, document and implement comprehensive procedures for the management of data, documentation and County property (equipment, hardware or software that belongs to County) in the Data and Property Management Plan (DEL-32).

APPROACH

The MBIS is a mission-critical biometric identification and storage system, housing highly-sensitive criminal information. It is being provided by Contractor with a high availability configuration running COTS hardware and software. Contractor will comply with all Safety (**Safety Rqt 1 and 2**) and Environmental Requirements (**Envrn Req 1 through 4**). All hardware procured by Contractor is commercially available through third party vendors and will adhere to the appropriate U.S. Underwriters Laboratory standards and will be installed according to the original manufacturer's recommendations including grounding.

Each client workstation will be delivered with a stand-alone UPS that is capable of powering continued workstation operations for a minimum period of 20 minutes after a power interruption. Contractor will configure the UPS management software installed on each client machine to notify the user in the event the System has been running on battery power for 10 continuous minutes. This will warn the user to shut down the machine to ensure no data is lost due to power failure. This software will automatically power off the System after running on battery power continuously for 15 minutes. This is to ensure that regardless of response to the user notification, the System will be shut down in a safe fashion and all data is saved prior to exhaustion of backup battery power.

All provided workstations are designed to fully adhere to the environmental design requirements for temperature, humidity and noise.

Data and property management best practices methodologies, as well as defined security provisions will be employed as part of Contractor solution to ensure that the MBIS is complete, secure, and operationally ready once deployed. Contractor is fully compliant with the CJIS security requirements and has recently passed a security audit at our primary system hosting facility. All data, whether in electronic or paper form, will be considered sensitive and addressed according to Contractor's, the FBI's, and LASD's security guidelines. These guidelines apply to all software, customer data, and System documentation produced or managed by Contractor under the contract (or procured by Contractor under the contract for the County system). These guidelines also apply to all data and documentation provided by County in the service of this contract.

TOOLS AND METHODOLOGY

Essential system processes, designed for the use and handling of County data, are considered to be of the utmost importance. System procedures will be documented for all equipment, software installation, System configuration, and backup methodologies for all sites. Password and physical access security will also be strictly enforced. These processes are designed to ensure that all hardware, software, data, and documentation are managed and secure. These processes adhere to best practices for data and property management and are currently employed within Contractor to ensure continuous operation and functionality.

The data and property management methodology is explained in detail in the following sections:

Physical Security

The physical security controls of the LASD Primary Site located in Norwalk, California and the alternate COOP Site will adhere to the same guidelines described within this document, while adhering to the CJIS Security Policy, CJIS Security Addendum, and LASD Security Policy.

All Systems and data Contractor stores, stages, or hosts are kept in our restricted access facility under camera-monitored, 24-hour security. All doors are secured by card key entry or key number access. All Systems in productive use, including all respective peripheral devices, all are fully secured. All software is kept under lock and key within the restricted facility fully compiling to CJIS security guidelines.

Technical Security Measures

The LASD System shall include the following technical security measures:

- Unique identification and authentication of terminals and users for all interactive sessions.
- Encryption for remote communications
- Security audit capability for interactive sessions and transaction based logging for message-based sessions. This audit shall be enabled at the system and application level.
- ORI identification and access control restrictions for message based access.
- System and data integrity controls.
- Access control on communications devices.
- For access from outside the CJIS firewall, Contractor provides, in addition to the strong passwords meeting FBI Security Police, FIPS 140-2 compliant encryption for data in transmission and data on the mobile device.

Mobile devices also use Contractor application level advanced authentication using fingerprint or face recognition or it can use the LASD enterprise advanced authentication.

Equipment – Hardware / Software Online Database

During staging and installation, all MBIS hardware and software will be logged into the Contractor Operations Database. Contractor will provide the County Project Team with hard copies of the equipment being transported and installed at the respective site. These hard copies will go with the respective equipment and serve as official signoff of hardware or software being delivered with respect to quantities. Once installed and inventoried at the Primary, COOP, and Remote sites, these documents are signed to show official receipt of delivery. Regardless of who the equipment belongs to, the documents will reflect ownership and history of installation and delivery.

The documents contain the following elements:

- Site locations, address, contact, phone number, and project number.
- Equipment Model, including attached peripherals and quantity.
- Hardware description, configuration, and quantity.
- Software description, configuration, and quantity.
- Terminal ID and IP address/subnet mask/gateway.
- Ownership of devices – hardware or software.
- Person who staged equipment, if applicable, with signature and date.
- Person installing equipment, signature, and date.
- Date installed, with customer date and signature.

Application Management

Applications managed by Contractor will have detailed documentation procedures to adhere to our data management procedures. This documentation includes patch management, application versioning, configuration management, backup/restore methodologies, and software loading instructions. These procedures will be followed for all applications deployed to the MBIS Primary Site, COOP Site, and the Remote Sites. All documents will be cataloged and stored in electronic form at the MBIS Primary Site. This comprehensive documentation will be available for review and audit by the customer at any time. In addition, all application changes will employ a fully documented change request process.

Data Management

All customer data including conversion data (electronic and hard card) or data to be loaded into the System via a specified process will be managed in a secure and timely manner. All customer data will have clearly documented instructions on the source of the data, what is to be done with the data, and when it is to be completed. The data will be logged when it arrives and when it leaves the building. At no time will data leave the secured Rancho Cordova facility until required to do so. All data will be returned to the customer and transported in a secured container. Backup copies will be made to address any risks in transporting electronic data and will be provided back to the customer upon written request. All data under Contractor management will be secured by physical room access and will be kept segregated until the data is ready to be used.

Database Backups

The following sections discuss the database backup and recovery strategies employed by Contractor.

Primary Site Database / Backup

Due to the importance of the data stored within the MBIS database, backups are performed on a daily basis using online backup scripts without human intervention. The ANSI/NIST file backup is performed using an incremental backup method where one portion of the files is backed up fully each night. This incremental backup process is also performed without human intervention. The backup saves are kept for three generations. Each backup generation contains one full week of backup tapes. The backup generations are recycled after the third week.

Oracle RDBMS is the key database engine for the MBIS database. With the Oracle automated backup software integration, the MBIS database will use the automated Oracle online backup feature effectively. The Oracle online backup feature allows completely uninterrupted System operation even during the backup process. The online backup capabilities not only permit transaction search processing to continue, but allow database updates (registrations, deletions) to occur while the backup is in progress. Due to the daily online backup methodology, the System will always be operational, ensuring that the backup process will not impact System uptime. The automated online backup methodology will be completely transparent from the user operations perspective. The backup process is initiated during non-peak workload hours through a preset scheduling function. The automated backup software checks for tape media availability, and checks to make sure that the appropriate "day" tape media is defined for reuse. The backup status is monitored and recorded so that detailed reports and filtered sample reports for troubleshooting can be produced. Other than the daily save, there are a number of backup measures recommended each year. These measures include internal disk image backups for servers and application backups that can be applied on a rotational basis. The purpose of these additional backup measures is to ensure smooth, efficient, and timely operation.

Primary Site System Recovery (Disaster Recovery – DR Solution)

In the event of an emergency arising due to system failure or natural disasters, Contractor will ensure continued operation of critical MBIS services. The LASD MBIS will be constructed in an Active-Active configuration. This configuration consists of two functionally independent systems that can each handle 100% of all daily transactions if required. In this Active-Active configuration, each site (Primary and COOP) will contain a complete copy of the LASD MBIS database, independent yet fully synchronized with each other and having the ability to support 100% traffic, should a System down situation arise. This configuration will provide full function and database registration capability no matter which System site is inactive.

A detailed COOP plan (DEL-22) outlining the procedure, policy, guidance and disaster response team structure to seamlessly handle any unforeseen disaster scenarios will be provided as a part of the RFP response package. A preliminary

COOP Plan is provided with the proposal. All recovery procedures, network connectivity, client switchovers will be performed and coordinated by qualified Contractor support engineers using predefined, verified, and comprehensive operational procedures.

In addition to the above, image, minutia, and Archive database backup generations are stored offsite in a locked box at a secure facility. Once per week, the oldest generation is delivered by a secure facility provider and signed for by the Contractor-LASD team. Currently, the most active generation is stored in the System tape library magazine with a second generation stored in our secured restricted-access facility for quick access retrieval.

Minutia Backups

System matching subsystem servers are designed to store fully redundant copies of all data. Additionally the MBIS systems will employ fully identical servers for enhanced throughput and availability. Minutia database (MDB) components stored on the matchers are loaded into the memory of each AIM matching subsystem during System startup. MDB components are also saved to internal disk to enhance System resiliency and startup time. All System configurations are backed up with third-party disk copy utilities and internal drives are further secured with the newest RAID disk technology.

MBIS Storage Data Backups

NIST records are stored internally as SQL database objects. External physical disk drives use the latest RAID 6 and cluster technology for data integrity and protection with round-the-clock monitoring. Database objects are backed up daily to alternate disk partitions and database backup files are then backed up to library tapes for secure storage.

Operational Life Cycle

Primary backups will occur during regular PM cycles. Complete image boot disks and external storage allow 100% copy of internal drive contents for quick restore in the event of a failure. Drive partitions are logical drives on physical disks which are RAID 6 protected with round-the-clock monitoring using hardware monitoring for failures. All drive partitions are backed up and all agency-only use partitions will be backed up once for structure only due to size/capacity.

Data Reporting Warehouse

All performance, statistical, or transaction-based data that is captured will be saved using the disk-to-disk storage standard disk-to-tape backup methodology, with weekly incremental saves. Contractor will retain 3 years of reporting data per the CJIS requirements with saves of data on an incremental, scheduled basis.

Online Help and Documentation

Online help files will be stored for two different purposes. Electronic user application guides will be provided in an online manner, whereby users may reference information for proper operation. System support and reference documentation will also be provided online to afford engineers easy access for efficiencies and support purposes. All access will be from Web URL or an internal application function, stored locally either on the workstation or at the Primary Site.

APPLICABLE STANDARDS

The following national and state standards are applicable for the migration of the data from the current existing AFIS system to the new MBIS system.

- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.

DELIVERABLE 2.1 – DATA AND PROPERTY MANAGEMENT

Contractor shall provide in accordance with Subtask 2.1 – Provide Data and Property Management the following Deliverable(s) for this component of the SOW:

- **DEL-32:** Data and Property Management Plan

SUBTASK 2.2 – IMPLEMENT SYSTEM SECURITY

Contractor shall implement a security program in compliance with the CJIS Security Policy referenced in Section 1.3.2 – Specifications, Standards and Guides above. All Contractor supplied facilities or systems shall provide protection and control of all County information, equipment, documentation and network access.

Contractor will comply with the requirements for implementing a security program in compliance with the CJIS Security Policy referenced in Section 1.3.2 – Specifications, Standards and Guides above as set forth in Subtask 2.2 – Implement System Security, which includes proposed activities, deliverables, descriptions of deliverable content, and media included as Attachment F to the proposal response to the MBIS Statement of Work.

DELIVERABLE 2.2 – SECURED SYSTEM ENVIRONMENT

Contractor shall document in accordance with Subtask 2.2 – Implement System Security its security program in an In-Plant Security Plan, as provided in the following Deliverable(s) for this component of the SOW:

- **DEL-10:** In-Plant Security Plan

TASK 3 – SYSTEM IMPLEMENTATION

Contractor shall implement, test and support County's Acceptance of the technology to be utilized in the provision of Work as provided in the System Requirements. All products, services and systems developed and/or delivered by Contractor shall comply with the System Requirements and the standards and guides set forth in Section 1.3.2 – Specifications, Standards and Guides.

Contractor shall provide all equipment and software necessary to satisfy the System Requirements at the proposed County operational Primary Site and the proposed Continuity of Operations Disaster Recovery site ("COOP Site"). Contractor shall provide all necessary equipment and software at Remote Sites to provide an equal level of service and functionality as replacement of all Existing System under the current BIS agreement, including, as applicable, servers, communications gear, workstations, printers and other equipment identified in the System Requirements.

Contractor shall provide County with a comprehensive set of user, system and management documentation. Contractor shall deliver those items identified in the list of Deliverables set forth in Attachment A.2 – Project Deliverables to this Exhibit A. Contractor shall provide the documentation in both electronic and hard-copy formats. All Deliverables shall be subject to County approval and Acceptance in order to satisfy the terms and conditions of the Agreement.

SUBTASK 3.1 – CONDUCT SYSTEM REQUIREMENTS REVIEW

Contractor shall conduct a System Requirements Review (“SRR”). Upon completion of the SRR, based on the results of the System Requirements definition activity, Contractor may recommend changes to the County System Requirements Specifications for consideration by County.

Contractor shall analyze County’s System Requirements and validate the requirements of the specifications. Contractor shall document the deficiencies in County’s System Requirements, if any, and recommend changes to the areas in which those changes would correct deficiencies or otherwise benefit the County (e.g., enhance the overall functionality, performance or reliability of systems or services; reduce costs; shorten the schedule; or reduce project risk).

Contractor shall document any recommended changes to County’s System Requirements Specifications and support these recommendations (e.g., with cost-benefit analyses).

Contractor shall provide to County with System Requirements Specifications and the rationale for any recommended changes. Contractor shall update County’s System Requirements Specifications with any changes resulting from actions assigned by County as a result of the SRR and all approved changes.

Contractor will comply with the requirements definition requirements of Subtask 3.1 – Conduct System Requirements Review.

This section describes Contractor understanding of the MBIS requirements and the approach to satisfying these requirements, including deliverables, descriptions of deliverable content, methods and tools to be used, and procedures to manage all functional and technical requirements throughout the Systems Development Life Cycle (SDLC) of the MBIS Project.

APPROACH

Contractor proposes to establish best practice Requirements Control techniques such as traceability, prototyping, modeling, impact analysis, and technical reviews to:

- Measure, report, and control changes to the solution requirements.
- Assess the impact of changes to the requirements on the project budget, schedule, resources, and risk factors.
- Manage ongoing changes to requirements artifacts attributes.
- Gathering and analysis activities will produce a first draft Project Management Plan (PMP, DEL-01).

After the System Requirements Review (SRR), the MBIS System Requirements Specification (SRS, DEL-02) will be brought under configuration management control.

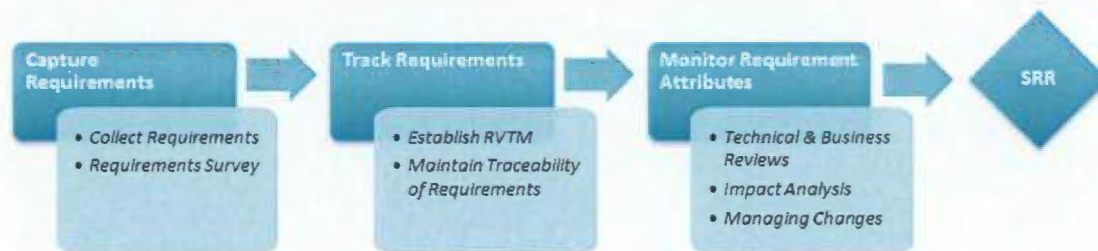
In post-award design discussions, Contractor will work with the County to establish the design and implementation details and document them in the LASD SRS (via the Requirements Verification and Traceability Matrix (RVTM, DEL-30) and potential change requests). During design discussions, Contractor will identify System design elements that will be brought forward from the legacy system, and focus on new design function considerations and changes that result in benefits to the proposed MBIS. At the SRR, Contractor will present the results of this requirements analysis.

Contractor will conduct the analysis and work with the County to develop the interface specifications for existing interfaces and new interfaces. Contractor will create the Interface Design Document (DEL-13) that results from this requirements analysis.

The Requirements Management approach, shown in Figure 1, defined herein will facilitate:

- A complete and precise set of documented solution requirements, consistent with the objectives of the approved MBIS project.
- Traceability of the solution requirements throughout the project life cycle, from beginning to end.
- Reporting on requirement attributes that facilitates management of MBIS requirements.

Figure 1: Requirements Management



Capture Requirements

LASD System Requirements Specification Document

Utilizing the LASD documented SRS, Contractor will review and analyze LASD's requirements to derive underlying System requirements and related functions. Any constraints to meeting stakeholder needs are identified. At this point, traceability between customer requirements and System requirements is established in the RVTM (DEL-30).

Requirements Survey

Contractor will analyze the MBIS SRS (DEL-02) and recommend implementation approaches that benefit the County in terms of schedule and functionality impact.

Contractor will provide the full list of recommended changes to the County at the SRR session with supporting documentation. Contractor will submit the design change recommendations (such as those above) to the County for approval and inclusion in the final MBIS SRS (DEL-02).

Track Requirements

Traceability of requirements ensures that the project meets the goal of converting LASDs business requirements to the specification, and ultimately to the solution itself. This also ensures that requirements can be evaluated during the project to maintain their validity in the System, or to adjust them accordingly. Traceability is maintained from the base requirements identified in the SRS (DEL-02).

Establishment of Requirements Verification and Traceability Matrix (RVTM)

Contractor will provide the RVTM (DEL-30) and use it for the following activities:

- Allocating stated and derived requirements to System components and/or other deliverables.
- Determining the source of requirements.
- Tracing concerns other than software that satisfy requirements, such as capabilities, design elements, manual operations, and tests.
- Locating affected System components when there is a requirements change.
- Recording requirement compliance.
- Traceability for System tests, ensuring all requirements are fully met.

Initially, Contractor will build the RVTM to contain all of the MBIS functional and technical requirements as defined in the requirements document.

Table 3 provides an overview of the initial information that Contractor will collect and maintain in the RVTM for every individual requirement.

Table 3: Requirements Artifact Attributes

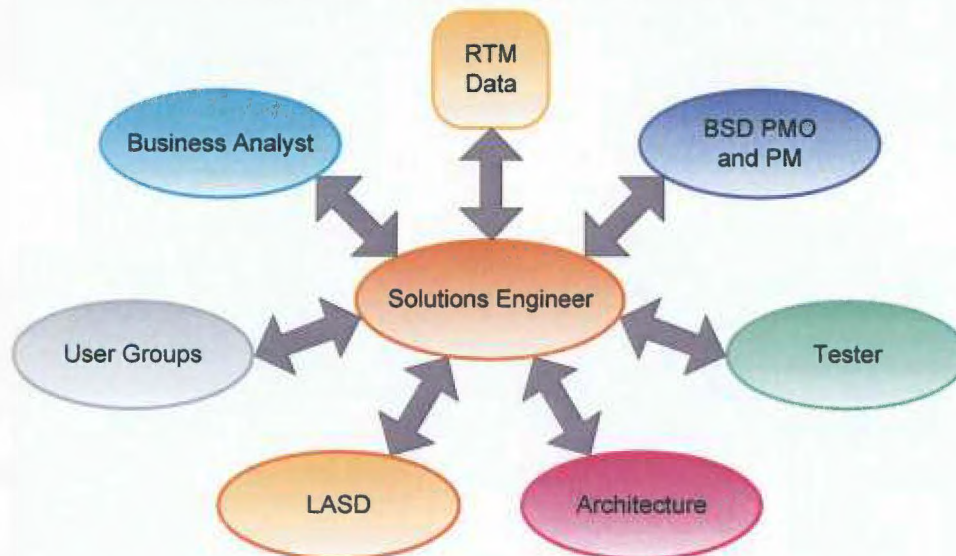
REQUIREMENTS ATTRIBUTES	EXPLANATION
ID	Unique identification number for this requirement.
Type	User or System.
Source	The source of the requirement (e.g., the RFP or Client Team).
Description	Clear, precise description of the requirement in definitive terms.
Design Doc Reference	Where the requirement is referenced in the systems design documentation.
Verification Method	The verification method that will or has been used to validate that each requirement has been satisfied (e.g., inspection, analysis, demonstration, test).
Test Phase	The current phase of testing for this requirement (e.g., Unit/Module Testing, Internal Integration Testing, System Testing, Factory Acceptance

REQUIREMENTS ATTRIBUTES	EXPLANATION
	Testing, System Acceptance Testing, User Acceptance Testing).
Test Case	Identifies the test case number.
Verification Problem	The criticality of any problems encountered during testing (e.g., Critical, Non-Critical, or Minor).
Problem Description Log	Chronological log of problem events.
Compliance	Yes/No.

Maintaining Traceability

Maintaining the integrity of the requirements stored in the matrix will consist of ensuring that the artifact attribute values correctly reflect the actual state of the artifact through the project life cycle. The Solutions Engineer is responsible for maintaining traceability of all functional and technical artifacts. As such, this role is the central hub and the authoritative source for all artifacts. Additionally, the Solutions Engineer interacts with various stakeholders whose day-to-day activities drive changes to artifact attributes as the project progresses, as depicted below in Figure 2.

Figure 2: Solutions Engineer Interaction



Monitor Requirements

Technical and Business Reviews

Contractor proposes that technical reviews be formalized to occur on a regular basis. The session will provide a format where elements of the solution can be explored from various angles, such as:

TECHNICAL	BUSINESS PROCESS	USER GROUP IMPACT
Infrastructure	Integration	Test results
Integration	Migration	Performance
Data migration		Usability

These review sessions gather both Contractor and County Subject Matter Experts (SME) from various project-related disciplines to discuss design and implementation progress and challenges.

Impact Analysis

Contractor proposes to perform a requirements impact analysis as required. The impact analysis will provide sufficient understanding to assess impacts to the project budget, technical design, resources, schedule, and risk factors.

Change Management

Contractor will track all functional and technical requirements in the RVTM (DEL-30). The RVTM will allow:

- End-to-end traces linking each requirement to related statements in vision or high-level design documents.
- Support for requirements change impact analysis through the identification of links made suspect by changes in requirements or in test and evaluation methods.
- Support for product acceptance, such as annotations recording the reason for changes to requirements and traceability from requirements to verification results.

TOOLS AND METHODOLOGY

- **Stakeholder Analysis** – During the Initiating Phase of the project, Contractor performs a Stakeholder Review. One objective of this review is to identify the stakeholders and their needs associated with the new solution. This information is used as an input to various Requirements Analysis tasks and techniques.
- **Interviewing** – This technique is used elicit information from the County for several purposes including to understand current business processes and rules, and validating the understanding of requirements.
- **Prototypes** – Wireframes or other prototyping methods may be used to confirm design requirements.
- **Use Cases** – Use cases may be prepared to document requirements for specific aspects of the solution.

ASSUMPTIONS

LASD and NEC project teams will be involved in system design discussions and interface control specifications to finalize the SOW, requirements documentation, and system design documentation after contract signing.

RISKS

Table 4: Requirements Definition Risks and Mitigation Strategies

RISK	MITIGATION STRATEGIES
Lack of project stakeholder involvement may lead to poorly defined statements of proposed requirements enhancements, leading to rejection as incorrect at the time of SRR.	Operational and technical stakeholders will be actively engaged from the start of the project to ensure adequate review of proposed updates prior to the SRR.
Scope creep can occur if requirement changes are uncontrolled.	The SRS will be placed under our formalized, documented project change control process to ensure only changes approved by LASD are implemented.

DELIVERABLE 3.1 – SYSTEM REQUIREMENTS SPECIFICATIONS

Contractor shall provide in accordance with Subtask 3.1 – Conduct System Requirements Review the following Deliverable(s) for this component of the SOW:

- **DEL-02:** System Requirements Specifications
- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes
- **DEL-30:** Requirements Verification and Traceability Matrix
- Change Request Documentation, as appropriate

SUBTASK 3.2 – PERFORM SYSTEM DESIGN AND DEVELOPMENT

Contractor shall design and develop the System to satisfy the System Requirements Specifications [DEL-02] and meet the required standards specified in Section 1.3.2 – Specifications, Standards and Guides. Contractor shall design, develop and produce or procure all hardware, software and data components of the System, with the exception of the operational data that is to be provided by County.

Contractor shall, to the maximum extent possible, use non-proprietary hardware and software in developing and implementing the MBIS. To the maximum extent possible, equipment for Remote Sites recommended by Contractor must be available commercially from third-party vendors as well as through Contractor, subject to installation of MBIS Software, which shall be controlled by provider alone.

Contractor shall conduct a System Design Review (“SDR”) and present to County for approval. The System design shall:

- Be complete down to the line replaceable unit (“LRU”) level for all hardware items and through the computer software unit (“CSU”) level for all developed software;
- In the case of commercial off-the-shelf (COTS) software, be complete through the level of licensed software products (“LSP(s)”);

- Identify the functions performed by, performance required of and interfaces supported by each CSU (for developed software) and each LSP (for COTS software);
- Document the number and interconnection of all LRUs and identify the software components loaded on each LRU;
- Document the bandwidth, memory and throughput of each LRU;
- Describe the interfaces supported by each CSU, LSP and LRU;
- Specify any standards with which each CSU, LSP and LRU complies; and
- Include complete work flows for all operational user and administrative functions.

As part of the SDR, Contractor shall present evidence (e.g., results of analyses, computer model and simulation results, benchmark results and vendor-supplied specifications) to demonstrate that the design satisfies the requirements of County's System Requirements Specifications [DEL-02] and the required standards set forth in Section 1.3.2 – Specifications, Standards and Guides. Contractor shall deliver a Requirements Verification Traceability Matrix [DEL-30] documenting mapping between (i) the requirements contained in the System Requirements Specifications and the major subsystems or components of the design, and (ii) the requirements contained in the System Requirements Specifications and the methods of verification indicated in Contractor's response to the System Requirements Specifications set forth in Appendix C (System Requirements Specifications and Response Forms) to the RFP.

Upon successful conclusion of the SDR and written approval of the design by County, Contractor may begin development and/or procurement of System software and hardware.

Contractor will comply with the design and development approach requirements of Subtask 3.2 – Perform System Design and Development.

This section describes Contractor's approach to satisfying these requirements; including proposed activities, deliverables, descriptions of deliverable content, methods and engineering tools to be used, risks associated the proposed design solution and its mitigation strategies, and our plan for conducting the System Design Review (SDR).

PROCESS

The Contractor Biometric Center of Excellence in Rancho Cordova was created to provide our design and development team with state-of-the-art methods, tools, and standards to ensure quality applications are produced and are delivered on time. This Center of Excellence will continue to develop and manage the core applications and interfaces required to keep the County's System at the cutting edge of biometric technology.

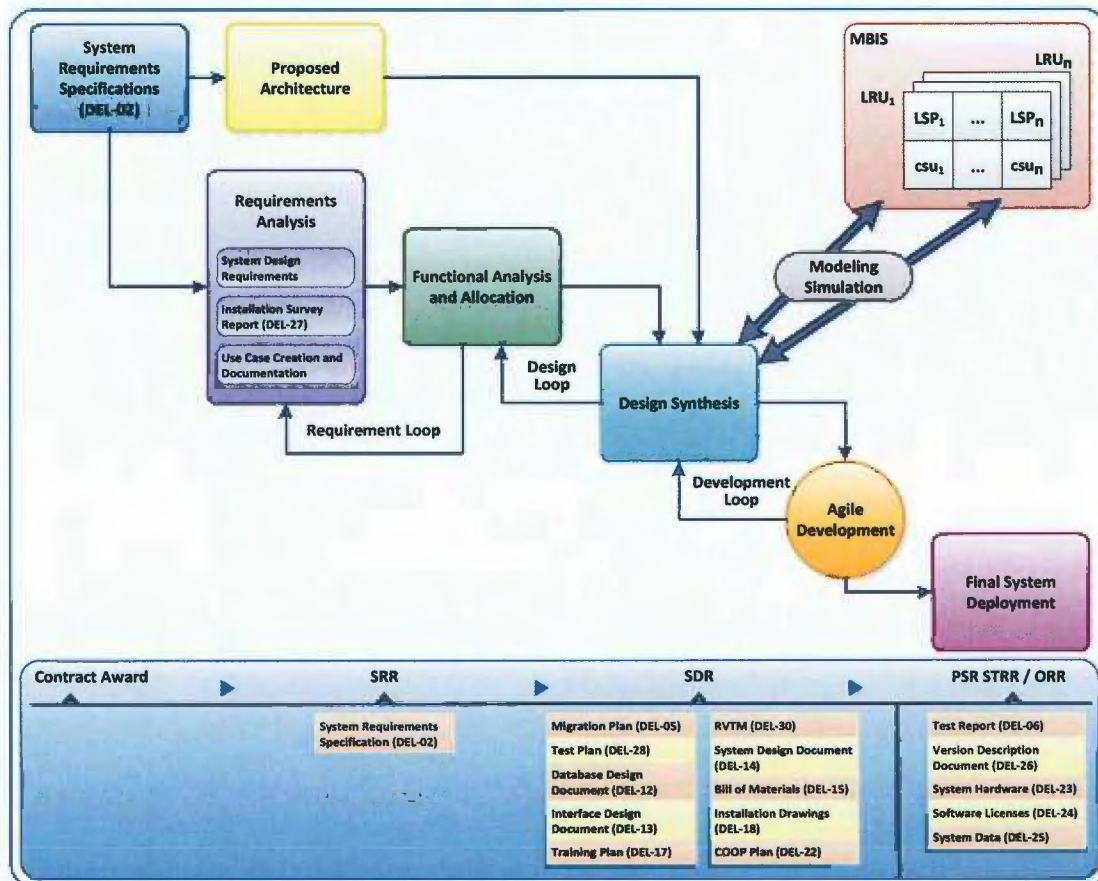
Figure 3 shows Contractor's design and development process to analyze the County's requirements, compare them to Contractor's current baseline product and existing interfaces, and integrate the changes required to satisfy the total System functionality

- Requirements Analysis – In this step, Contractor will capture the System requirements via comparison of all reference documents and information. Contractor will work with the County to establish the design details and capture the requirements in the MBIS SRS (DEL-02) document.

- **Functional Analysis and Allocation** – This step provides a detailed technical breakdown of the requirements, defines gaps against current baseline functions, and allocates the appropriate resources for additional development or integration needed.
- **Design Synthesis** – This provides the design structure and synthesis of required test cases, simulations, and models for development.
- **Agile Development** – The Contractor development and testing teams will use an Agile Software Development methodology for the MBIS implementation. This methodology is based on iterative and incremental development, whereby requirements and solutions evolve through each iteration.
- **Integration Testing** – The Contractor engineering teams integrate the base and customized components for rigorous testing in preparation for Factory Acceptance.
- **Timeline for Design and Development** – This phase is described in the Integrated Master Schedule (IMS, **DEL-03**) and will support the milestones, contract deliverables, and reviews Necessary for proper development, integration, and testing.

Contractor will design, develop, and procure all hardware, software, and data components of the MBIS to satisfy the requirements of the MBIS SRS and meet the required standards based upon the design and development process as depicted in Figure 3. Contractor will use non-proprietary hardware and software in developing and implementing the MBIS, to the maximum extent possible. All hardware and software installed (except for the MBIS software) will be non-proprietary and commercially available.

Figure 3: Design and Development during the Product Life Cycle



The Contractor solutions engineering and development teams will develop an architectural model for the proposed System, based on the SRS (DEL-02). The architectural model will include a complete list of System features addressing functionality, robustness, flexibility, and extensibility of the MBIS. This model will define the high-level organization of subsystems, define the interfaces between systems, determine the fit between existing assets and County requirements, and include a deployment model. From this model, the initial Database Design Document (DEL-12), Interface Design Document (DEL-13), and System Design Document (DEL-14) will be created in preparation for the SDR.

To ensure effective management of software, the system features will be grouped into subject areas and feature sets. Each feature set may include a combination of user interface, work flow, data management, and system interface features. This grouping enables an iterative and incremental development process. Adopting this type of development process provides a predictive and adaptive framework for the evolution of the proposed design solution into the fully-detailed design solution, and ultimately into the fully-realized deliverables.

For those features that Contractor needs to develop as additions to our core product, a detailed Unified Modeling Language™ (UML) model, including class and sequence diagrams, will be developed, forming the basis for the development of work package.

TOOLS AND METHODOLOGY

System architects and SMEs will regularly hold design review meetings throughout the implementation of the project. Including county SMEs in these meetings ensures that major architectural decisions are rooted in the County's business requirements. Contractor will document the system architecture using Microsoft® Visio®, UML, and ERwin® diagrams and other industry-standard authoring tools and manage the entire process using Microsoft Visual Studio® Team Foundation Server® (TFS) application life cycle and collaboration platform.

Internally, Contractor will hold daily stand-up meetings with implementation team members to raise issues, coordinate events, and update the team lead with the current status. This information is fed into the project plan and issues log.

Contractor integrates quality assurance activities directly within the agile project methodology. For the design and development, Contractor will conduct design and code reviews at the work package level. As each work package is delivered, Contractor will subject it to integration testing, function testing, regression testing, and performance testing. In order to decrease defect identification time Regression testing will be automated to the extent possible using HP Quick Test Professional (QTP). Contractor will record and manage defects and issues discovered through the testing process in TFS. The release of work packages will be governed by a change management process ensuring effective cross-team communication and coordination.

Table 5 provides additional information on the design and development tools used throughout our development life cycle.

Table 5: Design and Development Tools

DESIGN DEVELOPMENT TOOL	PURPOSE
Team Foundation Server	Team collaboration platform for application life cycle management. TFS is used extensively throughout the development process for: <ul style="list-style-type: none">• Requirements Tracking• Task Assignment• Software Version Control• Developer Code Review• Build Integration Process• Test Plan Management• Software Defect Tracking
Visual Studio	Software design and development studio. <ul style="list-style-type: none">• Application Development• Web Development• Interface Development• Software Debugging• Unit testing
Eclipse	Software Module Development <ul style="list-style-type: none">• Application Development• Work Flow Development• Interface Development• Software Debugging• Unit Testing
HP Quick Test Professional (QTP)	Automated Testing <ul style="list-style-type: none">• Application function testing• Regression Testing
Visio	System diagramming and modeling <ul style="list-style-type: none">• UML Diagrams• Functional relationships• Hardware and network layouts
ERwin	Database design and modeling <ul style="list-style-type: none">• Database visualization• Design generation• Standards definition

System Design Review (SDR)

Contractor will conduct the SDR in conjunction with County and present the design decisions from this review to County for approval. Contractor will document the complete work flows and designs in the system design documents, which will be complete down to the line-replaceable unit (LRU) level for all hardware items and through the computer software unit (CSU) level for all developed software or licensed software products (LSP) for COTS software. The design will identify the functions performed by, performance required of, and interfaces supported by each CSU (for developed software) and each LSP (for COTS software). The design will document the number of LRUs, how they are connected, and identify the software components loaded on each, along with the bandwidth, memory, and throughput requirements. The design will describe the interfaces supported by each CSU, LSP, and LRU and specify any standards with which each complies. At SDR, Contractor will present evidence (e.g., results of analyses, computer model and simulation results, benchmark results, and vendor-supplied specifications) to demonstrate that the design satisfies the requirements of the MBIS SRS (DEL-02), and the required standards.

RISKS

NEC realizes that risks are inherent to any development implementation. The identification of these risks and implementation of proper mitigation strategies help to ensure a successful project completion. Table 6 illustrates some of the high level risks associated with system design and development process.

Table 6: Design and Development Risks and Mitigation Strategies

RISK	MITIGATION STRATEGIES
Poor or inadequate requirement definitions	Collaboration with the County SMEs during initial design discussions to ensure all System requirements are captured.
Additional unforeseen requirements discovered during development process	Use Agile Software Development Methodology to allow flexibility and minimize impact, utilizing a formal change management process.

DELIVERABLE 3.2 – SYSTEM DESIGN AND DEVELOPMENT

Contractor shall provide in accordance with Subtask 3.2 – Perform System Design and Development the following Deliverable(s) for this component of the SOW:

- **DEL-05:** Migration Plan
- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes
- **DEL-12:** Database Design Document
- **DEL-13:** Interface Design Document
- **DEL-14:** System Design Document

-
- **DEL-15:** Bill of Materials
 - **DEL-17:** Training Plan
 - **DEL-18:** Installation Drawings
 - **DEL-22:** COOP Plan
 - **DEL-30:** Requirements Verification and Traceability Matrix.

TASK 4 – CONDUCT ACCEPTANCE TESTS

The MBIS is a complex software-based System that has many attributes that must be tested. Of critical concern is the appropriate test regimen to follow to ensure that all appropriate aspects are tested in a reasonable sequence. In order to understand the MBIS testing area, there is a need for a common vocabulary. The purpose of testing will be to verify that Contractor's product meets or exceeds all System Requirements Specifications [DEL-02].

Contractor shall develop and execute a comprehensive test program, spanning all phases of development and all levels of assembly of the system(s). Contractor shall develop a Test and Evaluation Master Plan (TEMP) [DEL-04], which shall:

- Govern all levels of testing, from the unit level through the fully assembled and integrated (with external systems) system;
- Govern all phases of testing, from unit testing through completion of System acceptance;
- Govern formal user acceptance testing; and
- Include the coordinated and complete testing with the Live-Scan Replacement equipment (subject of a separate but concurrent procurement) with the new MBIS, understanding that acceptance testing at each stage from Factory Acceptance Test through to User Acceptance Test will not be completed until Live-Scan and MBIS components are successfully tested together.

For unmodified COTS hardware and software, COTS vendor-supplied test results may be substituted for verification of requirements below the level of the fully integrated System.

Contractor will comply with the proposer test requirements of this Task 4 – Conduct Acceptance Tests.

This section describes Contractor's approach to satisfying these requirements; including proposed activities, descriptions of deliverable content, methods and tools to be used, risks inherent in the proposed test approach and its mitigation strategies. It also describes how the performance, interface safety, security, and standards requirements will be tested.

Beyond the required formal testing, Contractor also performs rigorous internal testing throughout the project life cycle. Details of our test process and methodology can be found in the Test and Evaluation Master Plan (TEMP, DEL-04), provided as Attachment B to this Business Proposal. The detailed specification of the testing types, standards, objectives, and resulting documentation are found in Section 2 of the TEMP.

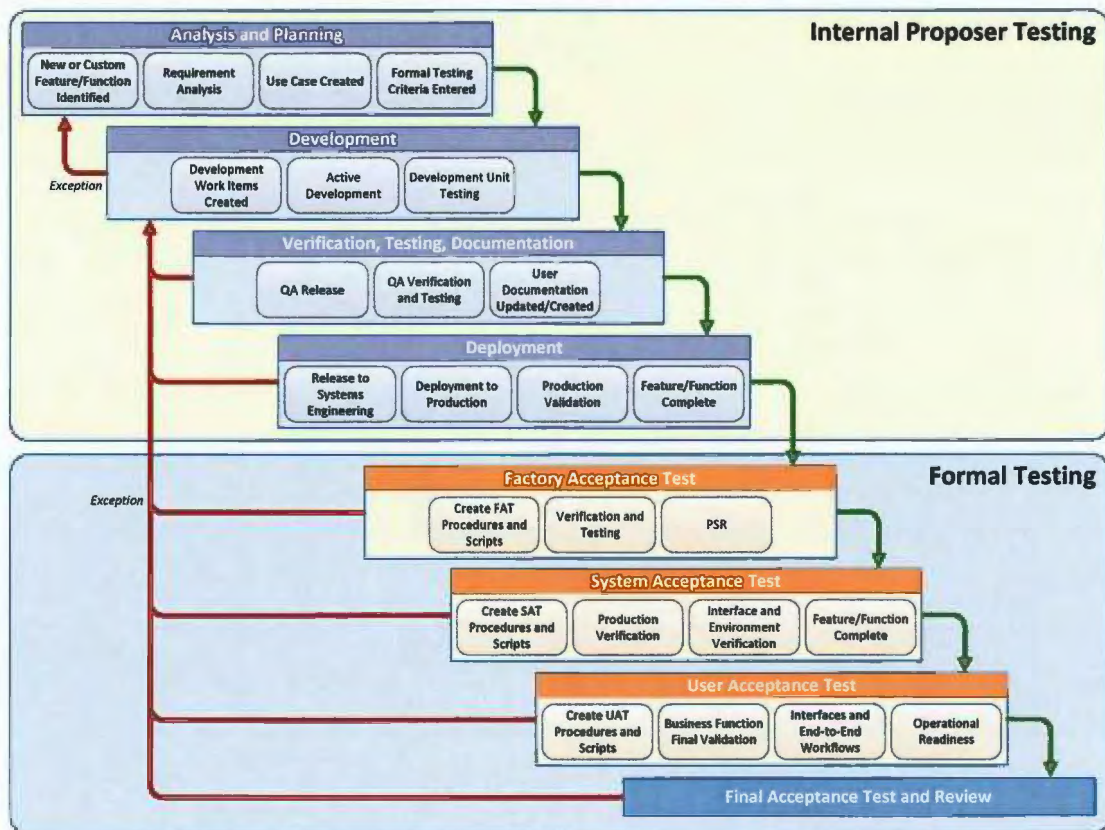
APPROACH

Contractor will develop and execute a comprehensive test program covering all phases of MBIS development and integration, as well as all system assembly levels. This plan is documented in the TEMP (DEL-04). The TEMP provides detailed levels of testing from the unit level through the fully-assembled system and governs formal and informal testing.

The major phases of testing as outlined in Figure 4 are:

- Internal Proposer Testing
- Factory Acceptance Test (FAT)
- System Acceptance Test (SAT)
- User Acceptance Test (UAT)
- Final Acceptance Test and Review

Figure 4: Contractor's Test Methodology



TOOLS AND METHODOLOGY

During testing, Contractor utilizes a series of test tools and simulators. These tools emulate functionality which may only be available in the production environment. Use of these tools mitigates risks when deploying the System by verifying that interfaces are functioning properly. The tool set utilized includes:

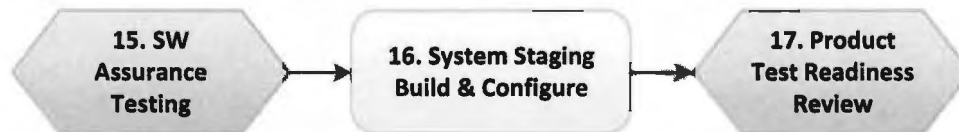
- **Live Scan Simulator** – This simulator acts as a Live Scan Device, submitting NIST files for tenprint processing. The tool is utilized when testing work flows, as well as used in performance testing by “stressing” the System.
- **WTester** – This tool emulates FBI and CCH interfaces. Submissions sent to the FBI or CCH are captured by this tool, allowing for canned or custom responses to be returned.
- **HP Quick Test Pro (QTP)** – QTP is utilized to script actions that a human may take in the System. For example, scripts exist which run manual tenprint operations. This tool is utilized to validate functionality in an automated manner, allowing testers to focus on interpretation and analysis.

Contractor firmly believes in assurance of quality before deployment. Extensive testing and validation require additional time in earlier stages of the project, which reduces risk and allows for a streamlined implementation.

Internal Proposer Testing

Internal proposer testing occurs during steps 15, 16, and 17 of the project life cycle shown in Figure 5 below.

Figure 5: Internal Proposer Testing During the Project Life Cycle



Internal proposer testing and verification are integrated from the initiation of a new or customized function and feature. Employing TFS as the primary tool, the process of maintaining traceability of the required function or feature is defined and audited. The item begins with the entry of a use case scenario, which is validated against the documented requirement. The use case includes the details of the requirement and the Necessary formal test criteria. This entry will move to development, where the specific development tasks are recorded as work items tied to the requirement. Once the development item has been unit tested, assignment of the item is transferred to the QA team, where software assurance, functional, integration, stress, and regression testing are performed. The item continues this testing cycle through the deployment of the feature/function. All modifications to the entry are logged with user name, date/time, and change made to provide a thorough history of the item. Custom load and interface simulators are used where needed to facilitate the informal testing. Informal testing uses a Contractor’s internal database in the test environment. After the informal testing has verified that all test cases are operating correctly, Contractor will conduct a Product Test Readiness Review (PTRR) and the process will move to formal testing with the FAT.

SUBTASK 4.1 – CONDUCT FACTORY ACCEPTANCE TEST

The purpose of the Factory Acceptance Test (“FAT”) is to ensure that the basic capabilities are available and work in a factory setting, and that the documentation associated with the System reflects the design and is usable (e.g., one typically uses the start-up and shut-down procedures to verify that they can be used, as written, to perform

the intended function). These tests are oriented toward verifying as much functionality, hardware, interface requirements, performance requirements, accuracy requirements and documentation as possible.

FAT is typically run with scripts to ensure agreement among the stakeholders on the input and expected results and that the tests are repeatable. After successful passage of the FAT at Contractor's facility, Contractor will be given permission to ship the System to the Operational Site(s).

The converted biometric database (known and unknown friction ridge files as well as related feature sets, pointers, and tables) will be audited as part of the primary site configuration FAT. Accuracy tests will employ these repositories, while the search records will be data sets prepared by County and having known image quality (tenprint only), minutiae counts (latents and their mates only) and mate or no-mate status information.

Contractor shall conduct FAT for the fully assembled and integrated System for both the Primary Site and the COOP Site (Disaster Recovery Site) levels. FAT shall include all tests Necessary to confirm that all requirements of the System Requirements Specifications [DEL-02] have been satisfied and to demonstrate compliance with required standards listed in Section 1.3.2 – Specifications, Standards and Guides. FAT shall also include all tests Necessary to demonstrate satisfaction of those requirements from any (provider-developed) subordinate specifications.

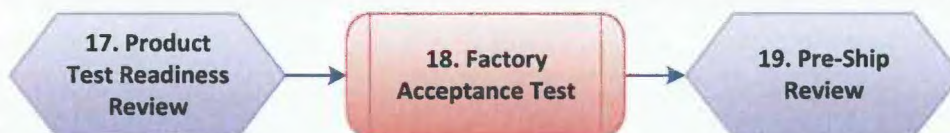
Contractor shall prepare a FAT Plan [DEL-28] and FAT Procedures [DEL-21] and submit them for approval. FAT shall be conducted in accordance with the approved FAT Plan [DEL-28] and FAT Procedures [DEL-21]. FAT may be conducted as a part of integration testing or as a separate phase of the test program, subject to County approval. Contractor shall conduct Product Test Readiness Reviews ("PTRR(s)") prior to the conduct of FAT. County will witness the execution of all FAT.

The results of FAT shall be documented in a FAT Report(s) [DEL-06]. Contractor shall conduct a Pre-Ship Review [PSR] to demonstrate the FAT success, to determine the readiness of the System(s) for delivery first to County's Primary Site and then secondly to the COOP Site and to secure County authorization to ship the System components and configurations.

Contractor will comply with the factory acceptance test requirements of this Subtask 4.1 – Conduct Factory Acceptance Test.

Factory Acceptance Testing (FAT) occurs during steps 17, 18, and 19 shown in Figure 6 below.

Figure 6: Factory Acceptance Testing During the Project Life Cycle



Contractor will conduct the FAT for the fully assembled and integrated System according to the FAT plan and procedures. The FAT ensures that basic capabilities and functionality are verified. The FAT will include all tests necessary to confirm that all

requirements documented in the SRS have been satisfied and demonstrate compliance with required standards. The FAT will consist of:

- Functional Test
- Repository Audit
- Performance Test
- Accuracy Test
- Documentation Suitability

FAT will utilize the Primary Site, COOP Site, and Remote Site equipment. This comprehensive testing will be supplemented with custom simulators and Contractor equipment to validate additional elements. The tools used will be the scripts designed to run the tests. The FAT will use the converted database. Results will be reported using the function checklists, accuracy checklists, and throughput results in the test report.

ASSUMPTIONS

Early stage of Quality Assurance testing is constrained to testing within the factory environment, providing for a unique set of risks as documented below. No assumptions are made; testing is performed for both positive and negative result cases. Not only is software tested for what it should do, but assurances and tests verify it does not do things it should not.

RISKS

Table 7: Proposer Test Risks and Mitigation Strategies

RISK	MITIGATION STRATEGY
The risks associated with the FAT are related to the interaction between the Primary, COOP, and Remote Sites – in particular, the communication that back end components have with external systems such as the FBI and criminal history systems.	Use of load and interface simulators that accurately simulate the external interfaces. The use of actual interfaces and network connections are utilized during the site acceptance testing to re-verify the interfaces.

APPLICABLE STANDARDS

As part of our internal testing process, Contractor adheres to the following standards:

- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- Electronic Biometric Transmission Specification (EBTS), NGI-DOC-01078-10.0.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.
- California Department of Justice (Cal-DOJ) Live Scan Transmission Standards

DELIVERABLE 4.1 – FACTORY ACCEPTANCE TESTING

Contractor shall provide in accordance with Subtask 4.1 – Conduct Factory Acceptance Test the following Deliverable(s) for this component of the SOW:

-
- **DEL-06:** FAT Test Report
 - **DEL-07:** Agenda
 - **DEL-08:** Presentation Materials
 - **DEL-09:** Minutes
 - **DEL-16:** Installation Plan
 - **DEL-17:** Training Plan
 - **DEL-18:** Installation Drawings
 - **DEL-19:** Training Materials
 - **DEL-21:** FAT Test Procedures
 - **DEL-22:** FAT COOP Plan
 - **DEL-26:** Version Description Document
 - **DEL-28:** FAT Test Plan

The following list represents the key deliverables from CONTRACTOR'S and the County for the FAT.

Further details regarding Factory Acceptance Testing (FAT) are provided in the TEMP.

Once the FAT testing is complete, the process continues with a Pre-Ship Review (PSR) and formal testing in the County environment with the SAT.

SUBTASK 4.2 – CONDUCT SYSTEM ACCEPTANCE TEST

The purpose of the System Acceptance Test ("SAT"), which is also known as System-level Integration Test ("SIT"), is:

- To demonstrate that the equipment was installed correctly and operates at the functional and performance levels verified at FAT;
- To verify the requirements that could not be verified at the factory (such as operations using a Remote Site's network);
- To verify the performance requirements (throughput, accuracy and reliability) with the full initial data load, multiple workstations, etc., to the extent that they have not already been signed off on at FAT; and
- To verify that the integrated sum, including Remote Site testing, is at least as functional as the sum of the individual parts and to verify that end-to-end work flows execute as anticipated – the actual verification of the correctness of the end-to-end work flows, to include all the processing at each step, is normally deferred to UAT.

The SAT is also script-based, with scripts built up from those used at FAT, ensuring that all additional requirements are allocated to specific test scenarios and that the scripts still ensure repeatability. Repeatability often requires cleaning out files and buffers that were changed as the result of a test step when the changed data is no longer needed by the System.

The SAT will include COOP activities. The minimum COOP activities that must be demonstrated include backing up and restoring data as well as using the COOP Site for primary processing, then restoring the entire System, ensuring that the repositories and

matchers are current and identical across the two sites. Verification of the COOP related procedures will be a critical part of the SAT.

Contractor will prepare the SAT Plan in cooperation with County. Contractor shall prepare SAT Procedures [DEL-21] and submit them for County approval. Contractor shall conduct the SAT in accordance with County approved SAT Plan and approved SAT Procedures [DEL-21]. Contractor shall conduct a System Test Readiness Review ("STRR") prior to the conduct of the SAT. County will witness the execution of all SAT(s).

Contractor shall document the results of the SAT in the SAT Report(s) [DEL-06]. Upon completion of the SAT, Contractor shall conduct an Operational Readiness Review ("ORR") to determine the readiness of the System(s), facilities and personnel to initiate the UAT and to secure County authorization to initiate operations.

Contractor will comply with the System test requirements of this Subtask 4.2 – Conduct System Acceptance Test.

This section describes Contractor's approach to satisfying the System Test requirements; including proposed activities, descriptions of deliverable content, methods and tools to be used, risks inherent in the system test approach and its mitigation strategies.

APPROACH

System acceptance includes both the SAT and UAT. The SAT begins the process of testing system functionality, throughput, and accuracy in the user environment and with the actual LASD networks and interfaces. The UAT continues with end-to-end business processes and work flows. This testing will verify operations using the County's production interfaces and networks.

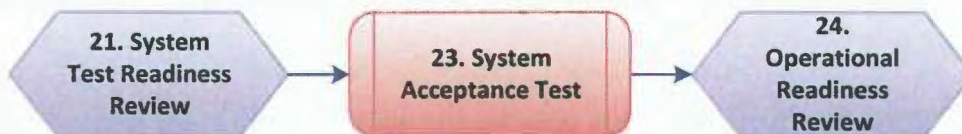
TOOLS AND METHODOLOGY

SAT is performed with the production system in place, utilizing live connections to all external systems. Testing methods are utilized to maximize user interaction. The preparatory stage of SAT is conducted to verify the production interfaces are active and properly integrated with the System. User training (step 22) is conducted prior to SAT, so that LASD personnel may participate and independently validate results.

SYSTEM ACCEPTANCE TEST (SAT)

The SAT occurs during steps 21, 23, and 24 of the project life cycle as shown in Figure 7 below.

Figure 7: System Acceptance Testing During the Project Life Cycle



The SAT will be performed using the Primary and COOP Sites plus the client equipment at a remote site. The SAT will be performed by Contractor personnel while being observed and monitored by County staff. The SAT will be a continuation and expansion of the FAT using scripts built up from the FAT. This process ensures validation of environmental issues is strictly compared to the Factory test results.

Contractor will conduct a System Test Readiness Review (STRR) prior to the SAT. Contractor will conduct the SAT according to a detailed System Acceptance Test Plan, test procedures, and checklists to document the completion of the tests. Contractor will create the test plan and the procedures subject to County approval. The SAT will have four components:

- Reliability Test
- Functionality Test
- Throughput Demonstration
- Accuracy Demonstration

The SAT will use load simulators for the throughput demonstration. The throughput demonstration will show any deviation between controlled factory testing and actual environment testing – validating the network architecture is sound. Accuracy is demonstrated to validate that no changes have occurred from FAT. Results will be reported using the function checklists, accuracy checklists, and throughput results in the test report.

Upon successful completion of the SAT, Contractor and the County will conduct an Operational Readiness Review (ORR) to certify readiness to move to the UAT and secure County authorization to initiate operations.

ASSUMPTIONS

It is assumed that the County will perform UAT in live, operational mode. No operational constraints exist for the UAT, excepting the availability of key County personnel during operations.

RISKS

Table 8: System Tests Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Impacting operations during test.	Perform simulations and dry runs to ensure ability to fall back if required.
Potential interruptions of site operations during SAT.	Minimize intrusive testing and set up fall back modes.
The primary risk of UAT is upon first utilization of the production interfaces and discovery of data dependent issues upon switchover.	The risk is mitigated by performing extensive interface testing during SAT. This testing requires the use of all permutations of data which may be received through the interface.

APPLICABLE STANDARDS

The TEMP (DEL-04) shall be adhered to for SAT and UAT.

DELIVERABLE 4.2 – SYSTEM ACCEPTANCE TESTING

Contractor shall provide in accordance with Subtask 4.2 – Conduct System Acceptance Test the following Deliverable(s) for this component of the SOW:

-
- **DEL-06:** SAT Test Report
 - **DEL-07:** Agenda
 - **DEL-08:** Presentation Materials
 - **DEL-09:** Minutes
 - **DEL-15:** Bill of Materials
 - **DEL-16:** Installation Plan
 - **DEL-17:** Training Plan
 - **DEL-18:** Installation Drawings
 - **DEL-19:** Training Materials
 - **DEL-21:** SAT Test Procedures
 - **DEL-22:** SAT COOP Plans
 - **DEL-26:** Version Description Document
 - **DEL-28:** SAT Test Plan

SUBTASK 4.3 – CONDUCT USER ACCEPTANCE TEST

The purpose of UAT is final validation of the required business functions and flow of the System, under real-world usage of the System by demonstrating that the delivered products and services are adequate for their intended purpose. UAT procedures will include both scripts and normal operations to see how the end-to-end work flows operate across the entire System, to include the interfaces to the California Department of Justice (“CalDOJ”). UAT will be planned to provide a realistic and adequate exposure of the System to all reasonably expected events. This includes things that might not happen in a normal period, such as a full backup and restore, switchover to the COOP Site and a full suite of report generation events.

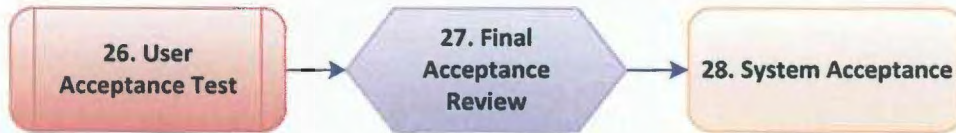
By this point in project, County and Contractor will have verified most or all of the accuracy, performance and capacity requirements. UAT will not be focusing on System problems (e.g., screening and reporting misspellings or software crashes), as those issues will be required to have been corrected by then.

Contractor will prepare a UAT Plan. The UAT Plan will be reviewed and approved by County. County staff will conduct UAT. Contractor shall provide the facilities, equipment and personnel to support the services identified in Phase 2 of this MBIS SOW during UAT. Contractor shall provide the facilities, equipment and personnel to analyze results of concurrent operations, to identify discrepancies between results of the legacy system(s) and results of Contractor delivered MBIS System(s), to resolve those discrepancies and, when those discrepancies result because of a failure of Contractor-delivered System(s), to meet the requirements, and to perform corrective maintenance.

Contractor will comply with the factory acceptance test requirements of this Subtask 4.3 – Conduct User Acceptance Test.

User Acceptance Testing (UAT) occurs during steps 26, 27, and 28 of the project life cycle as show in Figure 8 below.

Figure 8: User Acceptance Testing During the Project Life Cycle



The UAT is the final validation of System requirements and is run by County staff with support from Contractor personnel, as required.

Contractor will work with County staff to develop a detailed User Acceptance Test Plan, test procedures, and checklists to document the completion of the tests. The UAT tests business requirements and end-to-end work flows. The primary site UAT has two components:

- Business Functional Test
- Work Flow Functional Tests

Contractor will provide facilities, equipment, and personnel to analyze the results of the UAT and resolve any discrepancies found. Upon successful completion of the primary site UAT, the County will conduct a Final Acceptance Review (FAR). The UAT is performed without simulators for a true end-to-end test of the System and environment. The UAT will be run using the production database. Results will be reported using the UAT checklists in the test report.

APPLICABLE STANDARDS

The TEMP (DEL-04) shall be adhered to for SAT and UAT.

DELIVERABLE 4.3 – USER ACCEPTANCE TESTING

Contractor shall provide in accordance with Subtask 4.3 – Conduct User Acceptance Test the following Deliverable(s) for this component of the SOW:

- **DEL-06:** UAT Test Report
- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes
- **DEL-21:** UAT Test Procedures
- **DEL-22:** UAT COOP Plan
- **DEL-26:** Version Description Document
- **DEL-28:** UAT Test Plan.

TASK 5 – SYSTEM MIGRATION

The Subtasks below in this Task 5 – System Migration describe the migration requirements for the MBIS Operational Environment.

Contractor will comply with the migration requirements of this Task 5 – System Migration.

This section describes Contractor understanding of the migration requirements and our approach to satisfying these requirements, including deliverables, descriptions of deliverable content, methods and tools to be used, risks inherent in the proposed migration approach and its mitigation strategies. It also identifies the interfaces with County or other alternative sites that will be necessary to accomplish migration to the MBIS replacement and indicates how interoperability and continuity of operations will be maintained before, during, and after migration.

The primary objective of Contractor migration strategy is to provide a seamless transition from the County's current AFIS to the new MBIS. Contractor will transition the MBIS System in stages allowing agency operations to continue throughout the transition. Our plan will minimize the impact to the county and its users as they migrate from the current AFIS system to the new MBIS. The end result of the migration will be a MBIS platform that improves overall data integrity, provides additional system functionality, and improves overall System accuracy throughout the County.

Contractor has the experience and expertise to provide a successful, smooth, and seamless system migration. The conversion and migration of a MBIS data is a key part of system replacement. With Contractor as the supplier, it will be handled with the same planning and quality we have delivered to our customers for the last 25+ years.

APPROACH

The proposed MBIS design provides a comprehensive solution for the County's identification operations based on the RFP requirements. In addition to the system design additional considerations have been given to streamlining the data transition and system migration, reduce risks at each step of the transition, and to minimize the disruption in the agency's identification and investigation operations.

Contractor's detailed migration strategy will seamlessly and safely transition County and local law enforcement agencies to the new MBIS with no loss of service and minimal disruptions to the users.

This section describes Contractor's technical and management approach for site installation, legacy data conversion, and data load.

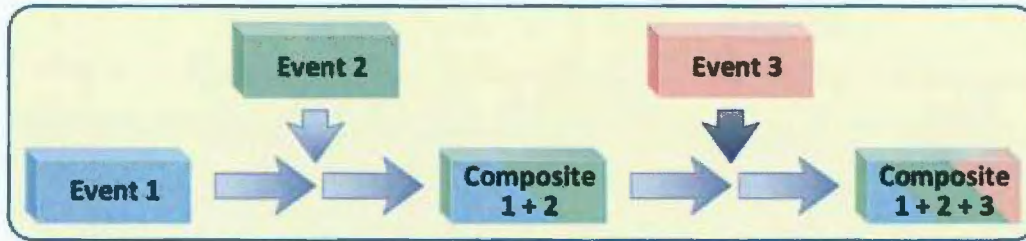
ANSI/NIST Tenprint Record Conversion

All ANSI/NIST records by the County will be processed, extracted, and loaded into the MBIS database as individual events linked to County MAIN ID. Each event will be fully accessible from the Archive web application and can be retrieved and printed at any time. For the purposes of registration to the matching system, additional migration processing based on finger and palm quality is performed to determine the records available. The following topics describe the additional finger, palm, and face processing.

Tenprint Identification Records

For tenprint identification match records, Contractor will build the best quality composite from all the available events. Contractor will compare NFIQ fingerprint qualities of for all registered events and determine the best quality set of roll and best quality set of plain impression prints. This single composite will be used for all identification matching. Figure 9 illustrates the process used in building the Identification Composite.

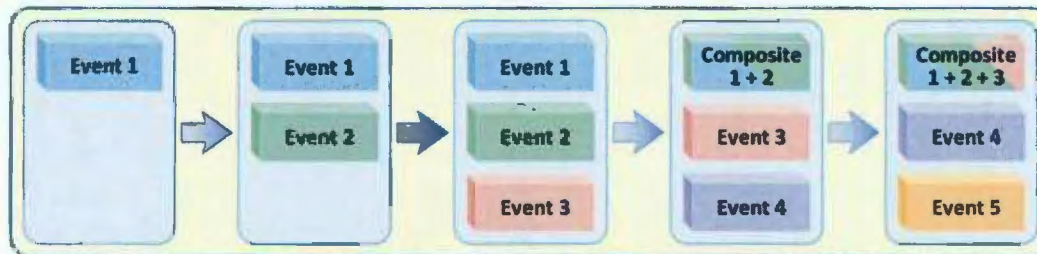
Figure 9: Tenprint Identification Composite



Tenprint Investigation Records

For tenprint investigation match records Contractor will utilize a hybrid event/composite structure for the matching database. The latent investigative records enrolled in the MBIS matcher will have up to three events – one composite event and the two latest events. For building the composite event, Contractor MBIS will compare fingerprint qualities for all registered events older than the most recent two and determine the best quality set of rolled and plain impression prints. This composite event will be created only when there are more than three events associated with an individual. Figure 10 illustrates the process used for the investigation search records.

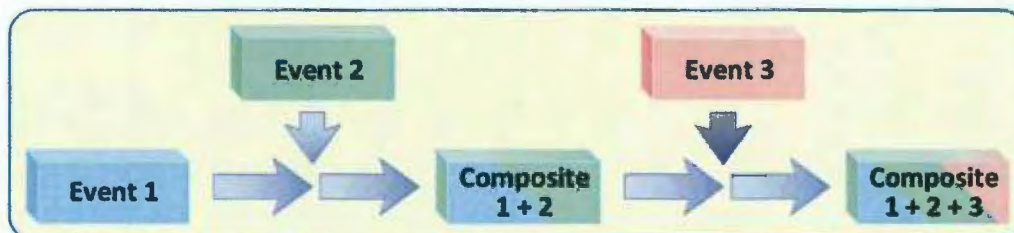
Figure 10: Tenprint Investigation Record Logic



Palm Print Investigation Records

For palm print investigation match records, Contractor will build a best quality composite from all the available events with palm print data. Contractor will compare Image Quality Library (IQL) palm print qualities and determine the best quality set of rolled and best quality set of palm print images, including full, upper, lower, and writer's images. This single composite will be used for all palm print investigation matching. Figure 11 illustrates the process used in building the Identification Composite.

Figure 11: Palm Print Investigation Composite



Facial Identification Records

For facial image identification match records, Contractor will use the most recent frontal face image for registration to the matching database.

Latent Record Migration

Contractor will fully transition all existing unsolved latent finger and palm records and place them into Contractor Integrated Latent Case Management System (LCMS). Although we would prefer to receive the unsolved latent records in ANSI/NIST formatted records with Type 9 EFS formatting, Contractor is fully capable of transitioning the unsolved database with other standard minutia encodings, or through the use of images alone.

Migration Searches

Contractor will perform a full cross search of all loaded tenprint records as part of the initial data load. The goal of the cross search is to allow the County to review unanticipated matches and unanticipated miss-matches for potential record updates and consolidations. Possible data corrections identified during the cross search will be provided at the end of the searches in an Excel spreadsheet.

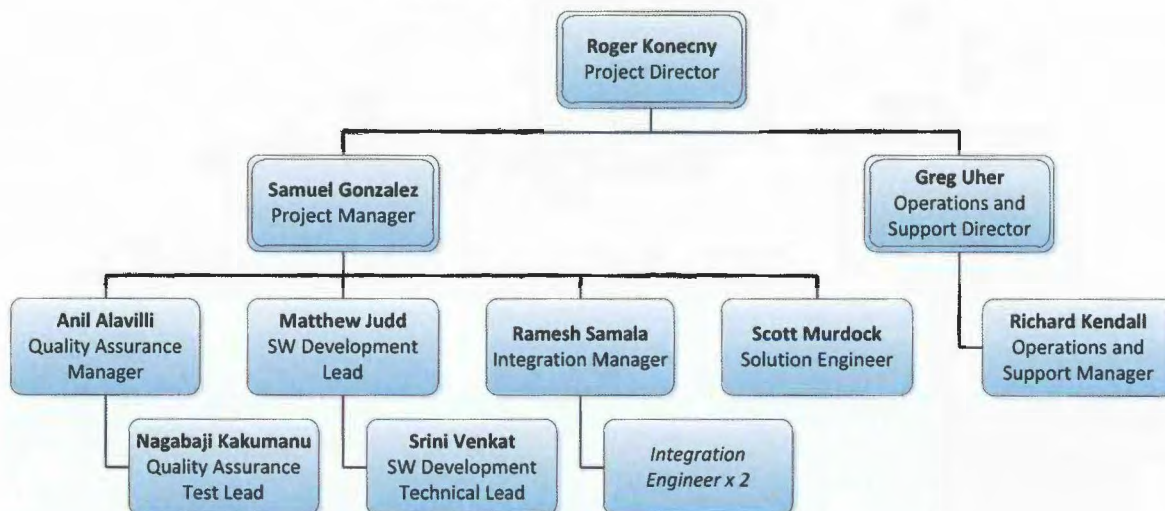
Contractor will comply with the requirement for reverse tenprint-to-latent and palm print-to-latent cross searches by performing forward searches during the migration process. Performing reverse searches would result in duplication of forward searches and extend the data migration time. The duplication is due to the fact that the algorithm for reverse searches generates the same results as the forward searches. Also, the reverse searches typically generate a very large number of results. The same information will be contained in the forward search results in a more compact format and in much smaller numbers.

Contractor will perform the latent fingerprint (forward) searches and latent palm print (forward) searches when the tenprint-to-tenprint de-duplication searches are completed. Possible hit results will be provided at the end of the searches in an Excel spreadsheet.

Migration Team

The migration team will be intimately involved in the design of the new System. They have all been directly involved in the migration of multiple MBIS Systems including ANSI/NIST and latent image conversions like the one for LASD. They have intimate knowledge of the data formats, tools, and procedure required to transition your current AFIS to Contractor's MBIS platform.

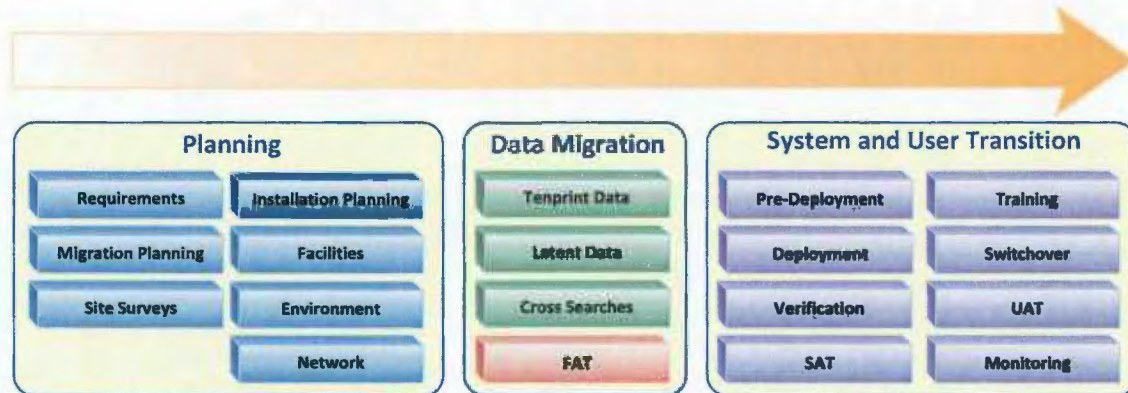
Figure 12: Migration Team



Migration Activities

Migration is divided into unique phases that encompass all parts of the data migration and system transition. Figure 13 shows the different activities involved in the migration process.

Figure 13: Migration Activities



The following subsections detail the steps performed during each phase.

Phase 1 – Site Surveys

The first phase in the MBIS data transition will be to perform site surveys of all sites with installation of MBIS equipment. Surveys will be performed by Contractor's Engineering staff and will allow for full accounting of the facilities layout, power, and network requirements.

Table 9: Phase 1 – Site Survey Steps

STEP	DESCRIPTION
1	Conduct Site Survey of Primary Site. Items to analyze as part of the survey are <ul style="list-style-type: none"> • Site Layout • Space available • Heating/Air Conditioning requirements • Lighting • Electrical Power • Structural Loading • Physical Access • Network
2	Conduct Site Survey of COOP Site assuming we are using the county provided site. Items to analyze as part of the survey are <ul style="list-style-type: none"> • Site Layout • Space available • Heating/Air Conditioning requirements • Lighting • Electrical Power • Structural Loading

STEP	DESCRIPTION
	<ul style="list-style-type: none"> Physical Access Network
3	Conduct Site Surveys of each Remote Site. Items to analyze are: <ul style="list-style-type: none"> Site Layout Equipment location Network connectivity System compatibility
4	Prepare an Installation Survey Report (DEL-27) for each site to document MBIS requirements and identify incompatibilities between the new MBIS equipment and the facilities or networks. Additionally the Survey report will identify any required facilities or network modifications required at the site.

Phase 2 – Conversion Hardware Configuration

The next phase in the MBIS data transition will be the initial setup and configuration of all central site hardware at Contractor's CJIS secure data facility. Performing the initial hardware setup, configuration, and data transition at our facility simplifies the process by locating all the hardware in a single location. In addition expert staff can directly monitor the initial phases of the migration. In the final stages of the data transition the data synchronization between the primary and alternate data systems can be performed across the local network reducing the bandwidth and overall time required to complete the synchronization.

Figure 14: Conversion System

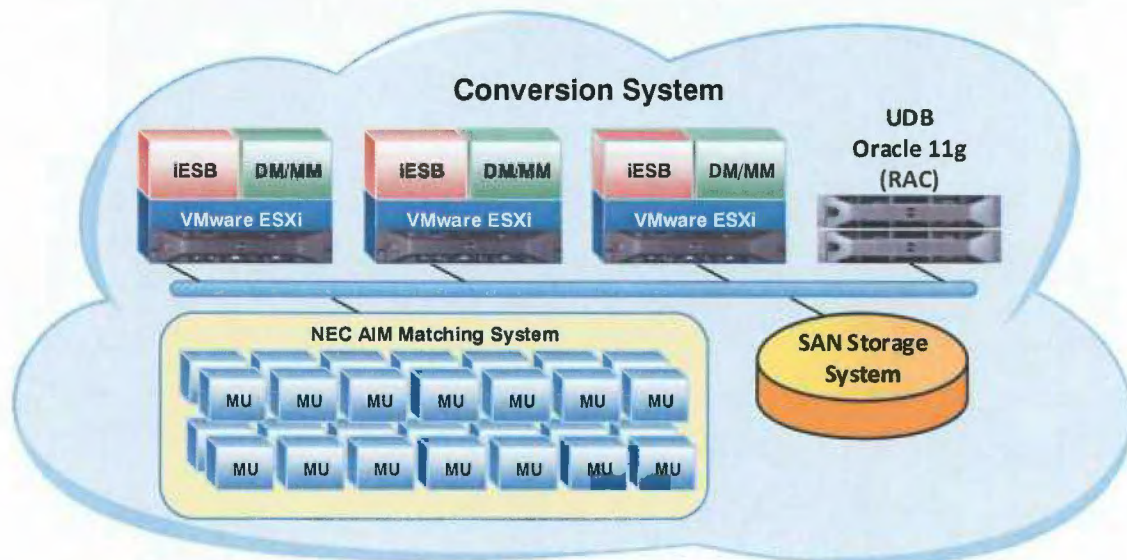


Table 10: Phase 2 – Conversion Configuration Steps

STEP	DESCRIPTION
1	The Primary site hardware required to support the project will be ordered and delivered to our CJIS secure transition facility.
2	The Primary site hardware will be set up and configured for data migration. In this phase, processing hardware from both the primary and COOP data center will be used to accelerate the data transition.
3	Data migration software tools will be installed on the hardware in preparation for the data transition.
4	Collection of data from multiple data sources including the current AFIS, Archive system, California Department of Justice, and other sources specified by the County will be received and prepared for transition into the new System.

Phase 3 – ANSI/NIST Tenprint Data Transition

The next phase in the MBIS transition will start the data conversion and will build and validate the Archive and MBIS identification and investigation databases. Data from the existing LASD Archive, AFIS database, California Department of Justice, and other specified sources will be loaded into the MBIS System, and cross searched against it to ensure data integrity.

Figure 15: Tenprint Data Transition

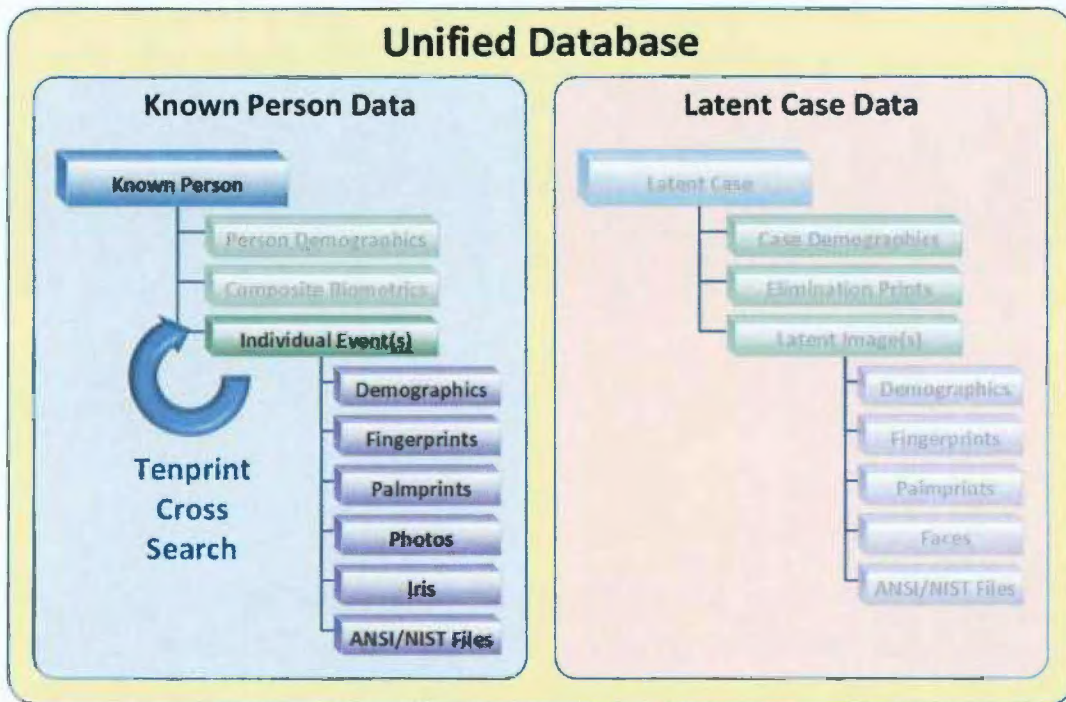


Table 11: Phase 3 – Tenprint Data Transition Steps

STEP	DESCRIPTION
1	<p>Load, extract, and register ANSI/NIST formatted data from existing LASD Archive, AFIS, and other County electronic record sources.</p> <p>The following steps will be performed on each ANSI/NIST formatted record:</p> <ul style="list-style-type: none"> • Process Fingerprint image data (all rolled and plain impressions) • Determine Quality using NFIQ and Contractor's IQL quality metric libraries • Extraction for Identification matching using Contractor's identification algorithm for both the rolled and plain impression prints • Extraction for Investigative matching using multiple extraction methodologies and multiple minutia formats to provide increased latent accuracy • Register to AIM matching database for cross check • Process Palm print image data • Determine Quality using Contractor's IQL Palm quality metric library. • Extraction of Palm print Minutia for Investigative matching using Contractor's Palm library • Register to AIM matching database • Process Facial Data • Extract frontal face images using Contractor's NeoFace libraries. • Register to AIM Matching Database • Process Additional Image Information • Convert ANSI/NIST Type 7 Record to Type 20 Record. • Convert ANSI/NIST Type 16 Record to Type 20 Record.
2	<p>Load, extract and register other electronic formatted records. If the County has electronic biometrics other than those in ANSI/NIST format Contractor will work with the county to develop additional conversion tools to load this data in the MBIS. Contractor can also format this date into ANSI/NIST compliant records and provide a copy to the County for future use.</p> <p>The following steps will be performed on other electronic biometric records. Depending on the biometrics present, not all steps may be taken.</p> <ul style="list-style-type: none"> • Process Fingerprint image data (all rolled and plain impressions) • Determine Quality using NFIQ and Contractor's IQL quality metric libraries • Extraction for Identification matching using Contractor's identification algorithm • Extraction for Investigative matching using multiple extraction methodologies and multiple minutia formats to provide increased latent accuracy • Register to AIM matching database • Process Palm print image data • Determine Quality using Contractor's IQL Palm quality metric library. • Extraction of Palm print Minutia for Investigative matching using Contractor's Palm library

STEP	DESCRIPTION
	<ul style="list-style-type: none"> • Register to AIM matching database • Process Facial Data • Extract frontal face images using Contractor's NeoFace libraries. • Register to AIM Matching Database • Create ANSI/NIST formatted record containing biometric data for future use.
3	<p>Perform cross search using extracted fingerprint data, for all converted events to look for the following information:</p> <p>Unanticipated matches against different County MAIN number. Identified records can be used to determine potential consolidations. All such matches will be noted and added to the conversion report.</p> <p>Unanticipated miss-matches against the same County MAIN number. Identified records can be used to determine potential wrongful associations. Information on potential matches may help identify the correct County MAIN number. All such miss-matches will be noted and added to the conversion report.</p> <p>All discrepancies found during the cross search will be documented and included in the detailed conversion report.</p>
4	<p>Save two copies of each ANSI/NIST file processed by the MBIS data conversion to external media for later delivery to LASD.</p>

Phase 4 – Tenprint Record Composite and Matching Registration

During this phase, the qualities of the biometric data loaded during the previous phase of the transition will be reviewed and used to build a best quality composite record for the purpose of identification and investigation matching. Once composite building is complete all tenprint data will be loaded to the matching sub-system.

Figure 16 depicts the data transition that will occur during phase 3.

Figure 16: Tenprint Composite Build

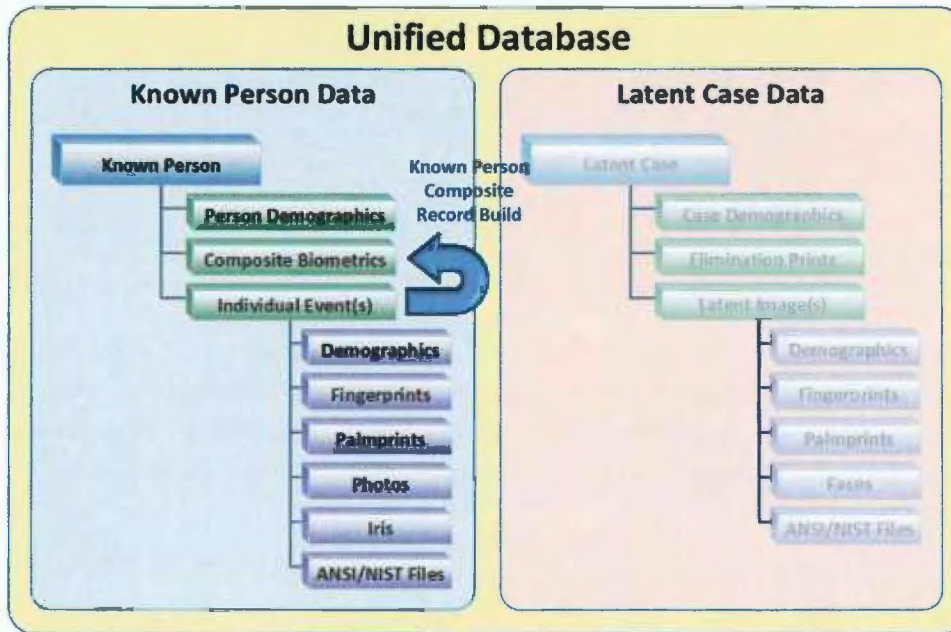


Table 12: Phase 4 – Tenprint Composite Build and Matching Registration Steps

STEP	DESCRIPTION
1	Compare fingerprint qualities of the rolled and plain fingerprint impressions for all registered events and determine the single best quality set of roll and plain impression prints for creation of a best quality composite for identification matching. Create tenprint composite record in the database with association to all contributing fingers.
2	Compare fingerprint qualities of the rolled and plain fingerprint impressions for all registered events older than the most recent 2 for determining the best quality set of roll and plain impression prints for investigation matching if available. Create latent composite record in the database with association to all contributing fingers.
3	Register the best quality roll and plain impression tenprint composite records to the AIM matching database.
4	Register the templates for the two most recent events as well as the templates for best overall latent composite created in step 2 to the AIM matching database.
5	Populate person level demographics based on rules decided during system design. Specific information that should be properly configured are the County MAIN ID, State of California's CII number, FBI Number, Person Name, Person DOB, Person Gender, etc. Potential sources of data for composite demographic information include: Individual event records County AJIS system through data export Other County systems not directly tied to the MBIS through data export.

Phase 5 – Latent Data Transition

During this phase, the Latent biometric data will be migrated to the MBIS and a forward search against the known person database will be launched. By using Contractor's high accuracy multi-extraction/multi-template latent encoding, Contractor foresees the County to be able to solve a number of cold cases.

Figure 17: Latent Data Transition

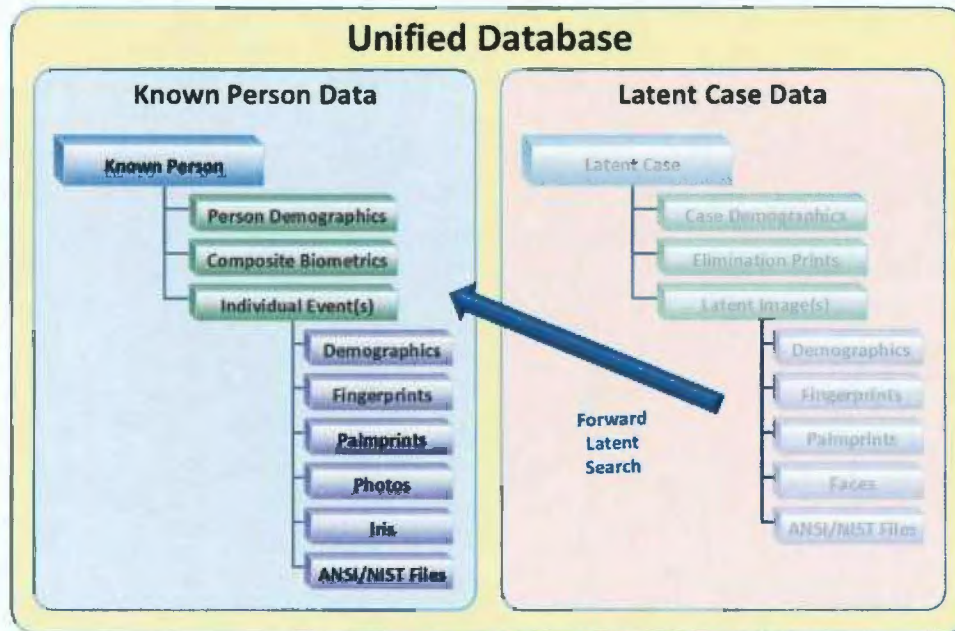


Table 13: Phase 5 – Latent Data Transition Steps

STEP	DESCRIPTION
1	<p>Collect unsolved latent data including both fingerprints and palm prints. The unsolved latent data for use in the migration may come from several different sources.</p> <p>Existing County latent data in ANSI/NIST formatted records with Type 2 Demographic data, Type 7 or Type 13 Image data, and Type 9 Minutia data in EFS Standard format. (Preferred)</p> <p>Existing County latent data in ANSI/NIST formatted records Type 2 Demographic data, Type 7 or Type 13 Image data, and Type 9 Minutia data in legacy FBI IAFIS format.</p> <p>Existing County latent data in ANSI/NIST formatted records with Type 2 Demographic data and Type 7 or Type 13 Image data.</p> <p>Latent image files in 8 bit grayscale in standard image formats.</p> <p>Contractor has the added benefit of providing access to the latent fingerprint and palm print from the AFIS repository of the California Department of Justice. We can electronically import these records from CAL-DOJ to the MBIS in Contractor native minutia formats and add to the unsolved latent database.</p>
2	<p>Convert existing Latent fingerprints. During this step, Contractor will take the existing latent fingerprint images in provided formats and load into the LCMS within the Unified Database. Depending on the original data format, different</p>

STEP	DESCRIPTION
	processing steps will be taken to ensure the highest quality latent encoding. At the end of the conversion process the following minutia formats will be encoded for each source image. Contractor proprietary multi-template minutia set. FBI standard EFS formatted Type 9 minutia template
3	Convert existing Latent palm prints. During this step, Contractor will take the existing latent palm print images formatted either as ANSI/NIST compliant packages or as individual image data and load into the Unified Database and matching system. Depending on the original data format, different processing steps will be taken to ensure the highest quality latent encoding. At the end of the conversion process, the following minutia formats will be encoded for each source image. Contractor Palm multi-template PC3R encoded minutia template FBI standard EFS formatted Type 9 minutia template
4	Perform a forward search of all unsolved latent templates including fingers and palms against the matching database built in Phase 4. All potential mate candidates discovered will be provided in the conversion report and can be prepared for manual verification by the originating agencies when the System goes live.
5	Save two copies of each ANSI/NIST file processed by the MBIS data conversion to external media for later delivery to LASD.

Phase 6 – FAT System Configuration

Once the System data transition is complete, the hardware components will be arranged into their final configuration and the System will be prepared for the FAT.

Figure 18: FAT System Configuration



The following table details the steps taken in Phase 6.

Table 14: Phase 6 – FAT System Configuration Steps

STEP	DESCRIPTION
1	All hardware will be fully distributed into the data center configurations at both Primary and COOP Sites each sized to reach 100% of the peak transaction processing volume.
2	A full database backup of all data migrated will be performed. This allows the full background database to be used for the FAT, but all data changes performed during the test can be rolled back ensuring full integrity of the migrated data.

STEP	DESCRIPTION
3	The Primary Site System and a number of workstations will be loaded, configured, and tested in preparation for the FAT.
4	Two-way synchronization will be established between the Primary Site System and the COOP Site System.
5	The FAT will be performed by test team members.
6	The Primary Site and COOP Site Systems will be packed up and shipped to the final destinations where they will be installed.
7	Primary Site and COOP Site System synchronization will be reestablished and verified.

Table 15: Phase 7 – System Deployment Steps

STEP	DESCRIPTION
1	Receive System hardware at County sites, unpack, install, and test to ensure System functionality.
2	Establish connectivity with the COOP site and re-connect Active synchronization process to ensure data replication between systems.
3	<p>Perform integration testing with the County systems to ensure full connectivity with the following County, State, and Federal Systems:</p> <ul style="list-style-type: none"> • CAL-DOJ Automated Fingerprint Identification System (AFIS) • FBI IAFIS • County Live-Scan System • Countywide Warrant System (CWS) • County Automated Justice Information System (AJIS) • County Mug Shot System • Mobile ID
4	<p>Perform catch-up conversion of all tenprint and unsolved latent data registered since initial data capture. In addition to the standard conversion steps covered above the catch-up data will be subjected to the following additional searches:</p> <p>All Tenprint records will be reversed searched against the unsolved latent finger, and unsolved latent palm databases to identify any known person associated with an unsolved latent record.</p> <p>All Latent records will be searched against the Known finger and palm databases for identification of known person associated with a catch-up unsolved latent record.</p> <p>Any known persons identified through the catch-up process will be identified and added to the conversion report and can be prepared for manual verification by the originating agencies when the System goes live.</p>
5	Prepare System for the SAT.

Phase 8 – System Switchover

This phase covers the final transition of all system processing to the new MBIS.

Table 16: Phase 8 – System Switchover Steps

STEP	DESCRIPTION
1	Contractor will work with County to determine a system switchover date. On this date the following system switchover steps will occur: County will stop forwarding of all Live-Scan transactions to the current AFIS. Perform final catch-up of ten print data to the new MBIS Forward all Live-Scan transactions to the new MBIS and return to normal tenprint operations At this point, automated tenprint processing will be completely transitioned to the new MBIS. System operations will be closely monitored to ensure a successful transition and stable operations have been established.
2	Initially latent operations will continue to process from current latent workstations on the existing AFIS. Latent workstation transition will occur in a staged manner allowing full rollout to the County while minimizing impact to the end users.
3	Contractor will coordinate with LASD to determine the order of remote site deployments. The Contractor installation teams will perform the MBIS replacement at each site will involve the following steps: New latent workstation will be installed at remote site and connected to the MBIS. Previous AFIS workstation will be removed. Latent Catch-up will performed for the latents processed by the remote site system since switchover. Once these steps are complete full latent processing including registrations can be re-initiated.
4	Contractor will establish a secondary support team for follow on support of the remote deployments after the initial installation. This will allow the installation team to move on to additional installations while providing full support of the users of the new system during system switchover.

Migration Plan Changes

The Migration Plan (**DEL-05**) will be considered a living document. Additional modifications to the plan may occur after contract signing. All changes and modifications will be noted on a Document Control Form (DCF), which will be located at the beginning of the document. The DCF is used as a management tool to maintain the integrity of the plan and to ensure that the requirements and specifications are executed correctly in the design and implementation of the solution.

APPLICABLE STANDARDS

The following national and state standards are applicable for the migration of the data from the current existing AFIS to the new MBIS.

- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- Electronic Biometric Transmission Specification (EBTS), NGI-DOC-01078-10.0.
- IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- California Department of Justice (Cal-DOJ) Live Scan Transmission Standards

Each of the subtasks below are addressed in the approach outlined above.

SUBTASK 5.1 – INSTALL SITES

Contractor shall conduct site surveys and analyses to determine the facilities requirements (e.g., heating, air-conditioning, lighting, electrical power, structural loading and physical access) for the facilities housing the replacement equipment at County's Primary Site, COOP Site and Remote Sites. Contractor shall review the network configuration at each Remote Site to ensure that the equipment to be installed is compatible with existing network topologies. Contractor shall document any incompatibilities between the MBIS equipment to be installed and the facilities or networks and identify in an Installation Survey Report [DEL-27] any required facilities or network modifications to be made by County.

Contractor shall prepare a Version Description Document with the complete instructions Necessary to install and configure all hardware, software and data associated with each deployment. The document will include site-specific installation information [DEL-27].

Contractor shall prepare an Installation Plan [DEL-16] to document the Necessary installation tasks, responsibilities, schedule, resource requirements, equipment layout, cabling and testing to verify correct installation of equipment and software at the Primary Site, COOP Site and Remote Sites. Contractor shall prepare Installation Drawings [DEL-18] to define equipment layout and cabling.

Contractor shall (subject to County approval) deliver and install the equipment and software deliveries at the Primary Site, COOP Site and Remote Sites. Contractor shall check the installation and perform the Necessary data conversions to prepare the equipment and software to support all testing and operations.

DELIVERABLE 5.1 – INSTALL SITES

Contractor shall provide in accordance with Subtask 5.1 – Install Sites the following Deliverable(s) for this component of the SOW:

- **DEL-16:** Installation Plan
- **DEL-18:** Installation Drawings
- **DEL-26:** Version Description Document
- **DEL-27:** Installation Survey Report

SUBTASK 5.2 – CONVERT AND LOAD DATA

Production of the Operational Database will involve: (1) the conversion of the legacy database and (2) the loading of this data into the Operational Database.

SUBTASK 5.2.1 – CONVERT EXISTING DATA

Contractor shall ingest and process all existing electronic tenprint, palm-print and latent records and convert (i.e., feature extract) them to the appropriate internal feature format. The latents shall be converted into the Extended Feature Set (“EFS”) format.

For electronic card images, if Type 7 and/or Type 16 data appears in the card image set, it shall be recorded as a Type 20 record.

Contractor shall convert friction ridge images (and some paper forms) into ANSI/NIST compliant image files and load them onto the System at the Primary Site with all appropriate transaction-related information, all available for search and retrieval based on ANSI/NIST and CJIS EBTs record types and field definitions.

Contractor shall perform feature extraction on all tenprint records for use in the matchers. Contractor shall cross-search all transactions to determine all transactions that share unique identities, link them together as single identities and assign a County Master ID (“MAIN”) to each unique identity. Contractor shall use any existing County person ID codes and the County MAIN and will retain all state identification (“SID”) numbers in indexing the tenprint repository. For cases in which new matches are found, the list of candidates shall be presented to County for review.

For cases in which three or more transactions are present at a state level for a subject, Contractor shall use the NIST Fingerprint Image Quality (“NFIQ”) software to quality-rate each finger image. Based on image quality scores, Contractor shall develop a “best image set” as a composite record for each of these identities at the state level. Contractor shall load feature sets for up to three transactions for each identity, the composite and the two most recent transactions, at the state level. The known tenprint file shall be loaded into the matchers for testing and Operational Use, with pointers to the appropriate transaction control number (TCN), SIDs and County MAIN.

For cases in which multiple palm transactions are present for a subject, Contractor shall use the most recent palm-print transaction based on the state that submitted it to extract features for the matchers for that state. After performing feature extraction on all palm records for use in the matchers, Contractor shall use any existing County person ID codes and the County MAIN and will retain all state SID numbers in indexing the palm-print repository at the state level. The known palm file shall be loaded into the matchers for testing and Operational Use, with pointers to the appropriate TCN, SID and County MAIN.

Contractor shall ingest all unsolved latent images and generate feature sets, either by auto-extracting them or by converting the corresponding existing feature sets to the EFS format. The preference is the use of the already encoded feature sets as the basis of re-encoding into the EFS format. The unsolved latent file shall be loaded into the matchers for testing and Operational Use, with pointers to the appropriate latent case numbers and related information loaded into the latent case management system.

Contractor shall preserve agency feature encoding through use of NIST Type 9 records saved by County staff to facilitate conversion to Contractor's feature set. If NIST Type 9 records are not achievable, Contractor's auto-feature function may be conditionally acceptable on the provided latent images, subject to County approval.

DELIVERABLE 5.2.1 – CONVERTED EXISTING DATA

Contractor shall provide in accordance with Subtask 5.2.1 – Convert Existing Data the following Deliverable(s) for this component of the SOW:

- Copies of converted Existing Data.

SUBTASK 5.2.2 – LOAD DATA

Contractor shall load all of the images and extracted features into the appropriate databases onto the System at the Primary Site and the COOP Site with the appropriate TCN, SID and County MAIN.

Contractor shall deliver two (2) copies of the output media for future use by County in any system or process of its choosing. As part of this task, Contractor shall:

- Cross-search all loaded tenprint records and provide a digital report of all possible unanticipated matches for use in consolidating records;
- Search all loaded tenprint records against the loaded latent records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record;
- Search all loaded palm-print records against the loaded latent records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record;
- Search all loaded latent records against the loaded tenprint records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record; and
- Search all loaded latent records against the loaded palm-print records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record.

At the end of the initial data load, Contractor shall produce a detailed report in accordance with the following requirements:

- The number of records converted, to include a count of modalities (fingers, palms, and Type 10 images) of the converted records.
- Any problems encountered, by record number (i.e., any conversion assigned number), TCN, problem type, and resolution.
- All records not successfully converted by record number and TCN, if available.
- Records that were identified as being from the same subject (i.e., multiple enrollments) sorted by TCN.
- Records that are forward or reverse searched and that are strong candidates for identifying latent impression sources.

- Average image quality for known tenprint by enrollment type, hand and finger position, by state, using the NFIQ tool.
- The results of a conversion audit.

DELIVERABLE 5.2.2 – LOADED DATA

Contractor shall provide in accordance with Subtask 5.2.2 – Load Data the following Deliverable(s) for this component of the SOW:

- Copies of data as noted above.

SUBTASK 5.3 – CONDUCT MIGRATION PLANNING

Contractor shall develop a Migration Plan [DEL-05] that identifies the activities, events and resources (tools, data, facilities, personnel and other resources) required to migrate from the LACRIS Automated Fingerprint Identification System (“LAFIS” or “Existing System”) to the replacement MBIS environment provided under the Agreement. The plan will identify the sources (i.e., Contractor, County or specific County Remote Sites) of all resources and specify when those resources will be required.

Contractor shall assist the County Remote Sites in planning their migration from the legacy AFIS system to the replacement MBIS provided hereunder.

ASSUMPTIONS

NEC has made the following assumptions as part of our migration strategy:

- All records for registration into the Known Tenprint TP, Known Palm KP, and Known Face KF MBIS databases are provided in ANSI/NIST format and conform to demographic (Type 2) specifications provided by the FBI or CAL-DOJ.
- The County has the ability to provide differential updates of the ANSI/NIST and latent export files after the initial data dump to allow for catch-up conversion and a staged system rollout without interruption to system end users.
- Cross searches utilizing records from the unsolved latent database will be searched using demographic filters (finger number, finger pattern, etc.) where available. The use of these filters will result in an Average Match Rate (AMR) of 50% of the full minutia database.

RISKS

The identification of risks and implementation of proper mitigation strategies help to ensure a successful migration. Table 17 illustrates some of the high level risks associated with the MBIS migration.

Table 17: Migration Risks and Mitigation Strategies

RISK	MITIGATION STRATEGIES
Delays in the Conversion Process	Monitoring of the Conversion Process – In the event conversion becomes prone to delay, consider the addition of hardware to increase the speed of conversion.

RISK	MITIGATION STRATEGIES
Unanticipated problems during Go-Live could impact operations at the point of cut-over.	<p>Onsite Support – NEC will have a support team at LASD at the time of cutover to answer questions, provide support and to immediately react to any issues that may be encountered. The NEC personnel assigned will have immediate access to third-level support personnel required to quickly resolve issues.</p> <p>Experienced Personnel – The NEC teams have both in-depth knowledge of large scale MBIS operations and connectivity to other systems, and also have experience in the cutover and migration of the databases.</p>

DELIVERABLE 5.3 – MIGRATION PLAN

Contractor shall provide in accordance with Subtask 5.3 – Conduct Migration Planning the following Deliverable(s) for this component of the SOW:

- Copies of converted existing data
- Copies of loaded data
- Conversion Report
- **DEL-05:** Migration Plan
- **DEL-16:** Installation Plan
- **DEL-18:** Installation Drawings
- **DEL-26:** Version Description Document
- **DEL-27:** Installation Survey Report

TASK 6 – CONDUCT SYSTEM TRAINING

Contractor shall develop User Manuals [**DEL-11**] addressing all user functions for all user types (e.g., tenprint and latent examiners, system administrators, maintenance personnel). User documentation shall describe the components, functions and operations of each server and workstation type. Operations descriptions shall include a list and description of all error conditions, as well as the associated error messages displayed and the action required of the operator for each error condition. Each MBIS workstation shall be provided with online user documentation that will be resident on the workstation or accessible via the agency's internal networks.

Contractor will comply with the training requirements of this Task 6 – Conduct System Training. Contractor's training team is intimately familiar with California type work flows. Targeted training facilitates a solution which meets the LASD organizational objectives.

This section describes Contractor's approach to satisfying the training requirements, including proposed activities, deliverables, descriptions of deliverable content, methods and tools to be used, risks inherent in the training approach and its mitigation strategies.

APPROACH

Contractor uses a hands-on approach to training that will keep LASD engaged and attentive. Contractor trainers are sensitive to varying learning styles and will ensure that content is delivered in a way that enables staff members to quickly implement new skills.

Contractor will provide the training and documentation that includes, but is not limited to, course outlines, course scopes, user guides, videos, computer-based training, and operator (technical) guides for all components of the LASD MBIS. The User Manuals (DEL-11) will address all functions for each user type and describe the components, functions, operations, for each workstation type. Contractor will offer onsite, hands-on training for users, technical operators, and system administrators. Historically, this has been shown to improve information retention so that users are prepared and comfortable when the LASD MBIS becomes operational.

TOOLS AND METHODOLOGY

As part of the Contractor training plan, we provide a complete documentation set that includes quick reference guides, user manuals in hard copy, electronic copy, and a fully-integrated online help system, which includes a list and description of all error conditions in addition to the action required by the operator for each error condition. The Contractor Support Engineer will maintain documentation required for the repair and maintenance of the equipment. Procedures will be documented in manuals provided with the prescribed training for operators, administrators, and managers.

Contractor incorporates extensive experience in its training program for the System. The course outlines—with Contractor course prerequisites, training location, and participation (number of students) as required by LASD (reference “Deliverable 6 – System Training and Materials” on page B-24 of LASD RFP Appendix B)—have been included in this response and will be further refined upon contract award to meet special training needs.

Each student will be provided a fully functional workstation and training database during the training sessions.

Training Courses

The following courses identify base curriculum for the MBIS primary courses: Tenprint Operator course, Latent Operator course, Archive course, LACRIS Help Desk course, and System Administration course.

- **Tenprint Operator Course** – Provides instruction on the preparation, input (data entry), search, verification, and disposition of automated and manual tenprint records. Topics covered include tenprint manual and automated work flow (fingers and palms), visual quality assessment, fingerprint and palmprint orientation, core/axis placement, pattern types and referencing, equipment operation, operational procedures, and transaction flow.
- **Latent Operator Course** – Provides latent examiners with instructions on the preparation, input, search, verification, registration, and disposition of latents and latent cases. Topics covered include, latent editing and enhancing, pattern types and referencing, equipment operation, and operational procedures. The course also provides instructions for case management and comparative analysis functions. Users learn case tracking, case and image history functions, case information reporting and access, image management, and image enhancement. This course also provides information on ULW jobs submitted to the FBI.

- **Archive Course** – Archive is a second-generation, web-based application that provides intuitive access to archived person records (by TID) and event records (by TCN), including demographic data, charge information, and images. The interface enables the user to perform simple and advanced searches. The Archive application also allows users to upload files of all types and relate uploaded files to specific person and event records. The Archive course provides users with the ability to retrieve and view fingerprint records, events, and documents.
- **LACRIS Help Desk Course** – Provides participants with an overview of the technical aspects of MBIS and provide methods to manage and resolve minor incidents quickly and effectively.
- **System Administration Course for Managers and Supervisors** – The administration interface is a new, web-based application that provides managers, supervisors, and/or system administrators responsible for overseeing day-to-day MBIS operations with tools for accessing and producing management reports, creating user accounts, managing work flows, monitoring servers, workstations, and jobs, performing audits and inquiries, and basic tenprint and latent operations.

DELIVERABLE 6 – SYSTEM TRAINING AND MATERIALS

Contractor shall prepare a Training Plan [DEL-17] and Training Materials [DEL-19] in accordance with Task 6 – Conduct System Training, including, via example, computer-based training, videos, guides and manuals, and conduct on-site user training as required to support testing, deployment and operations.

Contractor shall conduct four (4) types of courses as follows:

- **Tenprint Workstation Baseline** – This course will cover all MBIS tenprint functionality associated with the new MBIS. The course will provide hands-on instruction on the tenprint workstation for manual and automated tenprint processing. “Hands-on” requires that each student have access to a fully functional workstation and training database during the training sessions. This requirement applies to both the Tenprint Workstation Baseline training and the Latent Workstation Baseline training described below. The course will cover tenprint manual and automated work flows, displays, data entry, quality assessment and all functionality. In addition, the course will cover the basic and administrative user functions of the NIST archive. This course will also include the method by which NIST standard fingerprint transactions can be run against non-County member agency AFISs. This course will also cover palm-print and slap-print entry and quality assessment functions. This course will need to be conducted enough times initially to accommodate approximately 60 examiners and at least once yearly, for the duration of the Agreement, to accommodate up to 10 new examiners.
- **Latent Workstation Baseline** – This course will cover all MBIS latent functionality associated with the new MBIS. The course will provide hands-on instruction on the latent workstation and latent case management system. The course will cover latent manual work flows, displays, data entry, quality assessment and all functionality. In addition, the course will cover the basic user functions of the NIST archive. This course includes the method by which NIST standard latent transactions can be run against non-County member agency AFISs. The course will include instruction in best practices for ensuring optimum accuracy. This course will also cover latent palm-print and slap entry, quality assessment and matching functions. This course

will need to be conducted enough times initially to accommodate approximately 290 examiners and at least once yearly thereafter, for the duration of the Agreement, to accommodate up to 10 new examiners.

- **LACRIS Help Desk** – This course will provide an overall view of technical aspects of the MBIS and provide methods to manage and resolve minor incidents quickly and effectively. This course will need to accommodate approximately 12 participants initially and will need to be conducted, at least once yearly, for the duration of the Agreement, for approximately 12 participants, to accommodate new Help Desk personnel and keep existing staff current.
- **Managers and Supervisors** – This course will cover MBIS Management functions. The course will provide hands-on instruction on accessing and producing management reports, creating user accounts and performing audits and inquiries using the tools provided by the System.

Should County Remote Sites reasonably require additional training beyond that required above, such training will be provided at no additional cost to the County.

RISKS

Table 18: Training Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Operator Turnover	Re-occurring training is scheduled to be accomplished yearly.
Training Facility Readiness	Prior to training, the training manager will collaborate with the LASD and NEC project managers to ensure that the training facilities are fully equipped and ready for the different training courses.
Training Latency	The period of time between the training and productive use of the training may be of a duration causing lack of retention; NEC supplies initial training as concurrent to deployment as possible.

Contractor will provide the following deliverables:

- **DEL-17:** Training Plan
- **DEL-19:** Training materials
- **DEL-11:** User Manuals

TASK 7 – CONDUCT REMAINING MIGRATION TASKS

The Subtasks below provide the remaining elements that need to be addressed during System Implementation in order to complete the migration to the System.

SUBTASK 7.1 – MANAGE SYSTEM CONFIGURATION

County MBIS devices are geographically dispersed over a large area. This dispersion poses unique problems related to problem reporting; test, diagnosis and deployment of patches and revisions; and other aspects of configuration management. A Configuration Management Plan [DEL-29] and processes shall address these unique problems efficiently and effectively.

Contractor shall document and implement plans [DEL-29] for performing configuration control. Configuration control performed by Contractor shall accomplish the following:

- Establish a controlled configuration for each hardware and software component at the Primary Site, the COOP Site and each Remote Site;
- Maintain current copies of the deliverable documentation and code;
- Give County access to the documentation and code under configuration control; and
- Control the preparation and dissemination of changes to the master copies of the deliverable software and documentation placed under configuration control so that they reflect only approved changes.

Contractor shall generate management records and status reports on all products composing the controlled configuration for each hardware and software component at the Primary Site, the COOP Site and each Remote Site. The status reports shall:

- Make changes to controlled products traceable;
- Serve as a basis for communicating the status of configuration identification software; and
- Serve as a vehicle for ensuring that delivered documents describe and represent the associated software.

Contractor shall participate in County configuration control meetings. County configuration control meetings will establish and control the requirements baseline [DEL-02] throughout the performance of the Agreement and will control the operational baseline (deployed hardware, software, databases and documentation) once the MBIS becomes operational.

Contractor will comply with the configuration management requirements of this Subtask 7.1 – Manage System Configuration.

This section describes Contractor approach to satisfying the configuration management requirements; including proposed activities, deliverables, descriptions of deliverable content, methods, and tools to be used.

APPROACH

Contractor understands the complexities involved with administering and maintaining geographically dispersed systems. Contractor has the experience of handling successfully many MBIS implementations, which feature remote workstations that are not only geographically remote, but often have limited bandwidth connections to the Primary site. To address these challenges, Contractor shall centralize the software deployment and rollout. This along with the protocols and procedures outlined in the Configuration Management Plan (DEL-29) which will be submitted by Contractor, effectively and efficiently addresses the Configuration Management requirements for LASD.

Contractor's CM plan will apply technical and administrative direction and surveillance to perform the following tasks:

- Ensure the functional and physical characteristics of configuration items (CIs) are identified and documented.
- Control changes to CIs and related documentation.

- Record and report information needed to manage CIs effectively, including the status of proposed changes and the implementation status of approved changes.
- Audit the CIs to verify evidence of compliance to specifications, interface control documents, and other requirements.
- Provide traceability between “as-designed”, “as-built”, and “as-maintained” configurations.

For the LASD MBIS project, CM will acquire the necessary data from the engineering functions and provide for its secure storage; it is protected from unauthorized change, yet is readily available for use by technical staff. This is accomplished through the establishment of relationships between the various functional areas within the MBIS environments, as described:

- Systems Engineering – CM secures the master copies of configuration documentation and ensures that unauthorized changes are not made to this data.
- Design Review and Test – CM defines the system configurations and document versions required to perform specific design review, integration, and testing activities. The CM receives the review/test results generated.
- System Implementation – CM releases engineering data and configuration change status information on hardware and software required for site installation. System implementation provides feedback and problem reports to CM.
- Training, Support and Maintenance – CM exchanges data and status accounting information with the training, support, and maintenance functions to ensure their products are based on current and correct information. Manuals and training material must be of the correct configuration.
- Quality Assurance – QA provides CM with data gathered from the conduct of audits and process reviews, which will allow for the improvement of CM procedures.
- Document Management (DM) – The CM and DM functions work together to ensure data generated by the project is protected, secured, distributed in a controlled manner, and is readily available to technical staff.
- Security Engineering – CM ensures that security specialists are aware of all change activity occurring. The security specialists will provide data and change management feedback to CM to ensure all security processes, procedures, and requirements are being met. The control of change will help ensure security standards and policies are not violated and/or circumvented.
- Contracts – provides advice regarding any contractual implications of a proposed change.
- LASD Project Authority – CM provides LASD with visibility into the status of the technical data and any modifications.

Contractor’s comprehensive and rigorous approach will help meet all requirements for LASD and also mitigate any associated risks.

TOOLS AND METHODOLOGY

In order to effectively manage the MBIS CIs like

- **System** – System CIs are higher-level CIs used to group the hardware and software CIs that comprise the system.
- **Hardware** – MBIS Hardware CIs can be items such as; workstations, servers, scanner stations, etc.
- **Software** – MBIS Software CIs can be any software application or software application component used by the system. These CIs will be logically grouped in the MBIS Architecture.
- **Documents** – MBIS Document CI can be Scope of Work, BRTM, design documents, change requests, test cases, project schedules, size estimations, implementation documents, contract documents.

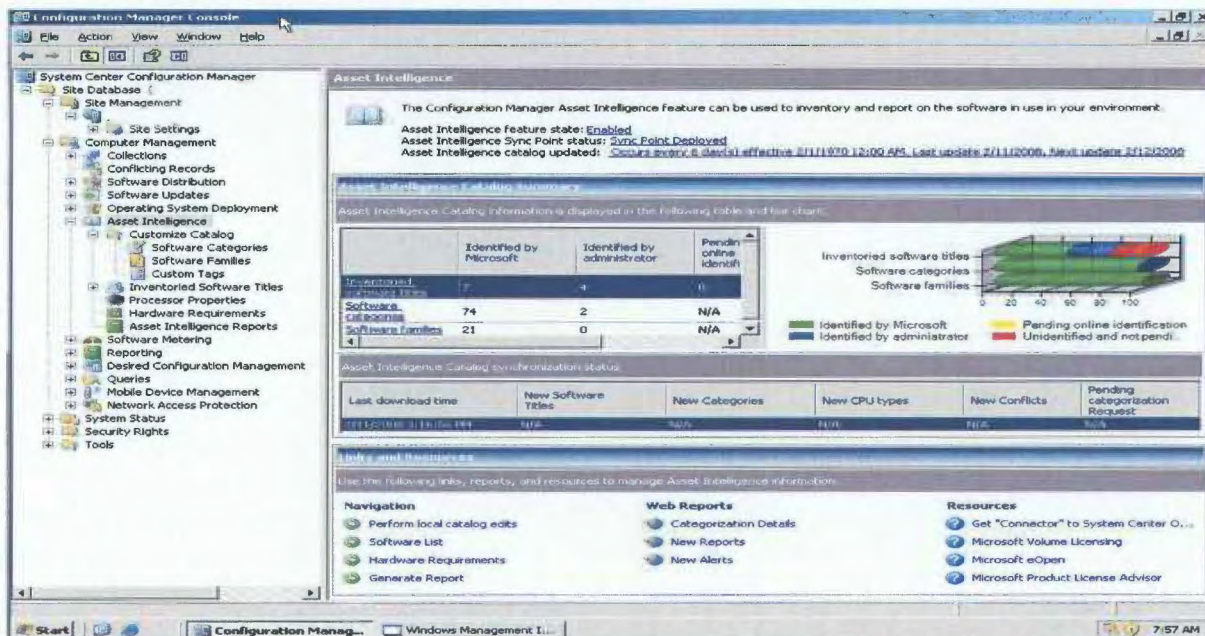
Contractors will utilize commercially available tools, described in the following sections, to help manage the system configuration for LASD MBIS project.

System Center Configuration Manager (SCCM)

SCCM is a Microsoft product which provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory.

SCCM enables the management and control of multiple configurations through the use of collections. This allows granular control of configurations at different sites, such as the Primary site and COOP site.

Figure 19: System Center Configuration Manager (SCCM) Console



SCCM allows for detailed analysis of deployment status, device and configuration management, as well as inventory capabilities. Access is provided through a client application for System Administrators. A web-based portal provides reporting, asset intelligence, and dashboard functionality. This allows for centralized automated control of the application versions and deployment.

Team Foundation Server (TFS)

Contractor utilizes Microsoft VTFS (referred to as TFS now on) to manage the control of software code and documents. This is Contractor's primary CM tool for defect logging, defect tracking, task management (task allocation, status update), source code control, build management, and release management.

TFS allows for detailed reporting on Software Quality, bugs and issues, task status, and software releases. TFS provides the following services:

- Release master copies of software for installation in target environments.
- Control of software, through the release of authorized software changes and the release of vendor revisions.
- Validates document deliverables against the associated software.
- Logs changes to controlled products.
- Generate backups and manage disaster recovery files.

Contractor utilizes TFS to record initial versions and manage changes to: business requirements; designs; work flows; procedures; documentation; hardware; COTS software; custom-developed software modules; conversion software; physical data base design; and application code.

The tools and methods being used allow Contractor to establish and maintain controlled configurations for the hardware and software components at the Primary Site, COOP Site, and Remote Sites. The unique problems that may arise due to County's geographic dispersion are addressed using these tools.

Throughout the life of the contract Contractor will provide comprehensive configuration management documents that will adhere to the county's deliverables and requirements.

Preliminary Configuration Management Plan (**DEL-29**) is provided with this proposal. This plan details how we meet the County's configuration management goals of:

- Establishing a controlled configuration for each operational hardware and software component at the Primary Site, the COOP Site and each Remote Site.
- Maintaining current copies of the deliverable documentation and code.
- Giving County access to the documentation and code under configuration control.
- Control the preparation and dissemination of changes to the master copies of the delivered software and documentation placed under configuration control so that they reflect only approved changes.

This plan is a living document and will be updated, throughout the engagement, with configuration items information. This plan will capture in-depth details that are sufficient to establish a controlled and planned release management of the deliverables.

Additionally, Site Installation Reports which specifically detail the following information will be prepared for the Primary, COOP, and each of the Remote Sites:

- Installed hardware

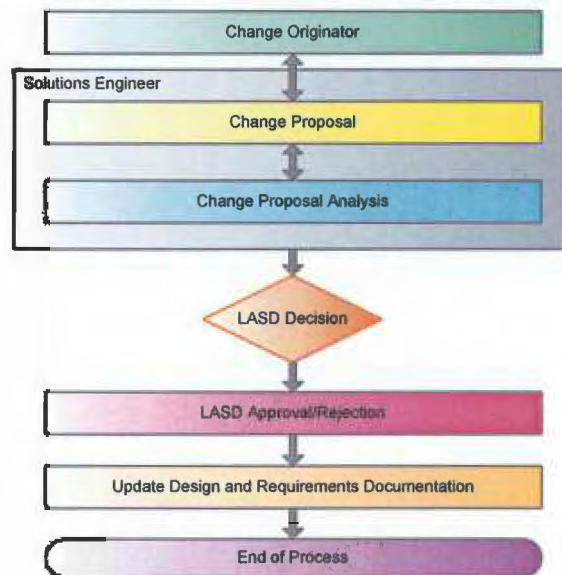
- Network connections
- Assigned IP addresses
- Current operating systems
- Installed middleware
- Installed Contractor software including details the currently installed release versions
- Diagrams showing hardware connections and locations

These Site Installation reports will be maintained and updated as the site configuration changes. These Contractor standard implementation documents, with their included change tracking, will meet the county's requirement for management and status reports regarding configuration control.

Finally, Contractor will prepare a Version Description Document detailing all deployment and installation instructions for all System components. This allows for full rebuild of the System solely from the description document.

Contractor will be an active participant in the County Configuration Control meetings throughout the implementation of this project and subsequently once the MBIS is operational. Figure 20 provides an overview of Contractor's standard configuration proposal process.

Figure 20: Configuration Change Proposal Process



RISKS

Table 19: Configuration Management Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Non-availability of Source Code	NEC utilizes a centralized source code repository (TFS) that maintains all versions and change history of the code under management. In addition this repository is backed up nightly to ensure all original source code is fully available even in the event of a disaster situation

RISKS	MITIGATION STRATEGIES
Un-authorized installation of applications	By using a centralized system control management platform (SCCM) and directory system, NEC administrators can control user rights, and control system deployments.
Unforeseen impacts of change requests.	NEC follows a complete change control management process which includes multi-level review of all proposed changes. This helps to identify potential conflicts and raise issues prior to requirements finalization.

APPLICABLE STANDARDS

- LASD RFP Statement of Work
- IEEE Standard 1058, Software Project Management Plans, Section 4.7.1 Configuration Management Plan
- IEEE Standard 828, Software Configuration Management Plans
- ISO 10007, Quality Management – Guidelines for Configuration Management
- EIA649, National Consensus Standard for Configuration Management

DELIVERABLE 7.1 – SYSTEM CONFIGURATION PLAN

Contractor shall provide in accordance with Deliverable 7.1 – System Configuration Plan the following Deliverable(s) for this component of the SOW:

- **DEL-02:** System Requirements Specifications
- **DEL-29:** Configuration Management Plan
- **DEL-26:** Version Description Document

SUBTASK 7.2 – CONTINUITY OF OPERATIONS PLANNING

Contractor shall perform the Necessary planning; deliver a plan (“COOP Plan”) [DEL-22]; provide or utilize the necessary facilities (e.g., the Sheriff’s data center in Norwalk, existing provider proposed infrastructure or Nlets (the International Justice & Public Safety Information Sharing Network) infrastructure), equipment, supplies, data and documentation; and conduct the training Necessary to establish a viable COOP Plan capability that ensures the performance of Contractor’s essential functions during any emergency or situation that may disrupt normal operations and leave the Primary Site facilities damaged or inaccessible.

The purpose of COOP planning is to assure that the capability exists to continue essential provider functions across a variety of potential emergencies as well as when maintenance or upgrade activities might impact MBIS System use. A COOP Plan should account for:

- Ensuring the continuous performance of County’s essential functions/operations during an emergency;
- Protecting essential facilities, equipment, records and other assets;
- Reducing or mitigating disruptions to operations; and
- Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

The COOP capabilities provided by Contractor under this Agreement shall be:

- Maintained as an active-active site;
- Capable of providing 100 percent of the MBIS services (in the event of the loss of the Primary Site) both with and without warning/scheduling; and
- Continuously operational in a load-balanced environment during normal operations.

At a minimum, the COOP Plan provided by Contractor shall contain the following:

- Plans and procedures
- Identification of essential functions
- Alternate facilities
- Interoperable communications
- Vital records and databases
- Tests, training and monthly exercises/drills.

The COOP Plan should be developed and documented to ensure that, when implemented, it will provide for continued performance of essential County functions under all reasonably foreseen circumstances. At a minimum, the COOP Plan shall also:

- Delineate essential functions and activities.
- Outline a decision process for determining appropriate actions in implementing COOP plans and procedures.
- Establish a roster of fully equipped and trained emergency provider and County personnel with the authority to perform essential functions and activities.
- Include procedures for employee advisories, alerts, and COOP Plan activation, with instructions for relocation to pre-designated facilities, with and without warning, during duty and non-duty hours. This includes providing for personnel accountability throughout the duration of the emergency and providing for continuous operational status in an active-active environment.
- Establish reliable processes and procedures to acquire resources Necessary to continue essential functions and sustain operations similar to that of the primary site for up to 30 days.

Essential functions are defined as those functions that enable Contractor to provide vital services, under any and all circumstances.

Contractor will comply with the continuity of operations (COOP) requirements of this Subtask 7.2 – Continuity of Operations Planning.

This section describes Contractor's understanding of the requirements and approach to satisfying the COOP requirements; including proposed activities, deliverables, descriptions of deliverable content, methods and tools to be used; and operation concepts for continuity and availability as they relate to the System design. It also describes approach for determining and evaluating the facilities, equipment, software, data, records, documents, personnel, and other assets that are critical to maintaining continuity, quality, and level of service. This section also identifies the constraints and assumptions used in deriving the COOP plan, risks inherent in the proposed COOP approach and its mitigation strategies.

The purpose of the COOP plan is ensure the continued operation of critical MBIS services in the event of an emergency arising due to System failure or natural disasters. It is designed to establish policy, guidance, and to ensure the continued operation of critical MBIS services in the event such a catastrophic scenario occurs. The System will be constructed in an active-active configuration. This configuration consists of two functionally independent systems that can each handle 100% of all daily transactions if required. In this active-active configuration, each site (Primary and COOP) will contain a complete copy of the database, independent yet fully synchronized with each other and having the ability to support 100% traffic, should a System down system arise. This configuration will provide full function and database registration capability no matter which System site is inactive.

The specific goals of the COOP are:

- Ensuring the continuous performance of County's essential functions/operations during an emergency
- Protecting essential facilities, equipment, records and other assets;
- Reducing or mitigating disruptions to operations; and
- Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

A detailed COOP plan (**DEL-22**) outlining the procedure, policy, guidance and disaster response team structure to seamlessly handle any unforeseen disaster scenarios is provided as a part of the RFP response package. This detailed plan provides substantiation of understanding and the viability of the approach.

As decided by County, the location of the COOP Site will be at Contractor's data center located in Rancho Cordova, California. This data center facility is fully equipped with environmental, electrical, and network infrastructure supporting the requirements of the MBIS hardware and software configuration. It is already staffed with highly-qualified technical personnel on a 24/7 basis. In addition, the data center is already CJIS compliant and has an established connection to the California Department of Justice.

APPROACH

The proposed MBIS configuration provides an Active-Active system implementation between the primary and alternate data centers with both systems designed to handle 100% of the County peak workload. All registered data will be continuously synchronized to ensure access to the same biometric data regardless of where search transactions are being processed. During normal operations the transaction processing workload will be distributed between both sites. This configuration ensures that there is no service degradation in the event that a network outage occurs between the Primary and COOP Sites.

During normal operations, the following activities will occur within the Primary and COOP Sites:

- Registered Data synchronization between the Primary and COOP Sites databases using the iESB Active-Active transaction synchronization.

-
- Two-phase commit mechanism for data synchronization to ensure that matching at either site will generate identical search results.
 - Configuration information and component versions (e.g., updates and patch levels) of the iESB service group are synchronized through VMware vCenter between the Primary Site and COOP Site Provisioning Systems.
 - Data backup of complete MBIS repository and matching subsystem with offsite storage providing for full data recovery in the unlikely event of a multi-site disaster.

Thus, the database and the configuration information between the sites' iESB components are continually in sync in terms of configuration, updates, and patch levels. More importantly, the all resources at both sites are being used continually for daily operations, and not merely in standby mode thus they are readily available for full operational load in the event of an emergency.

In a situation calling for the activation of the COOP, the following steps will be taken in the below mentioned order:

1. All High priority transaction processing for criminal booking and mobile ID searches from clients which are connected to the unavailable site, will be immediately re-directed to the active site.
2. Remote site workstations and clients will be redirected to communicate active site for all forward latent searches and reverse latent verifications.

Detailed failover and failback procedure is provided in the COOP Plan (DEL-22).

TOOLS AND METHODOLOGY

COOP Plan Overview

Contractor complies with the requirement to deliver a COOP Plan (DEL-22) before System Design Review (SDR) and its revision at Pre-Ship Review (PSR).

The COOP Plan contains the guidelines and criteria for making the determination to activate the DR plan. COOP plan also includes all aspects of disaster recovery, including the following COOP Items:

- Disaster recovery team organization:
 - Recovery management team
 - Operations team
 - Network team
 - Facilities team
 - Communications team
- Team tasks and responsibilities:
 - Immediate activities for each team following DR activation
 - Ongoing activities
- Details of recovery activities
 - Activities that must be completed as per the SLA.

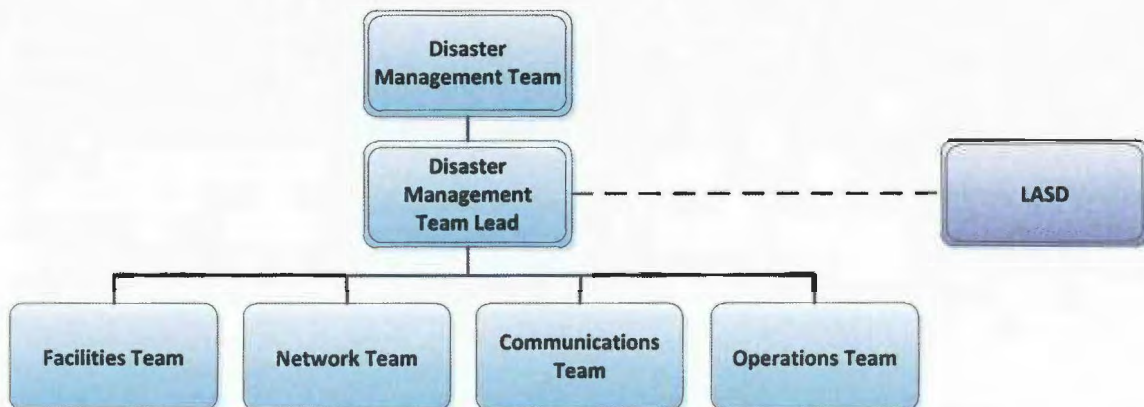
- Escalation procedures
- Design documents and Procedures
 - System design documents for services and database
 - Operation procedures of all components
 - Description of emergency procedures
 - Recovery scenarios
- Contact Information

Contractor's understanding of the essential services is as follows:

- Highest priority is for criminal booking, and mobile ID searches:
- All daily and peak hourly transaction workload and response time requirements as specified in the RFP are met immediately from the time of COOP activation.
- Second priority is for latent fingerprint and palmprint reverse searches.
- Third priority is for latent fingerprint and palmprint forward searches.

The plan is structured around teams, with each team having a set of specific responsibilities. It contains all the information Necessary to restore an operational service in the event of a serious disruption of MBIS services at the Primary Site. Figure 21 provides an overview of the Disaster Recovery team structure.

Figure 21: Disaster Recovery Team



The plan will be accompanied by signatures of each personnel in the distribution list to certify that the plan is read and understood.

ASSUMPTIONS

Contractor assumes that there will be sufficient network bandwidth between the Primary and COOP Sites. It is anticipated that database synchronization processes will be the dominant network traffic activity. Since approximately 20% (or more) of all daily transaction workload occurs during peak hours, it is possible that the hourly data size to be replicated to the alternate database will exceed the WAN connection bandwidth. Thus, depending on the available network bandwidth and peak hour workload, there may be a time lag in database synchronization. Contractor will be responsible for network connectivity from the Primary Site to the COOP site, located in Rancho Cordova, CA.

RISKS

Table 20: COOP Planning Risks and Mitigation Strategies

RISK	MITIGATION STRATEGY
Insufficient network bandwidth between the Primary and COOP Sites.	NEC will meet with the County IT team and conduct Site Surveys to ensure adequate network bandwidth.

APPLICABLE STANDARDS

Contractor adheres to best practices according to the following standards:

- Contractor disaster handling and recovery procedures are based on ISO/IEC 24762:2008.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.

DELIVERABLE 7.2 – COOP PLAN

Contractor shall provide in accordance with Subtask 7.2 – Continuity of Operations Planning the following Deliverable(s) for this component of the SOW:

- **DEL-22:** COOP Plan.

SUBTASK 7.3 – CONDUCT FINAL ACCEPTANCE TEST

Upon the successful completion of Subtask 4.3 – Conduct User Acceptance Test through Subtask 7.2 – Continuity of Operations Planning, County will conduct a Final Acceptance Review (“FAR”) to determine whether Contractor has satisfied the terms and conditions of this SOW and whether to accept the System for Operational Use. The determination will be based upon the Deliverables that comply with the requirements of the Agreement, the satisfactory performance of all SOW activities and the successful demonstration through the System Tests that the System and System Data satisfy the requirements of the System Requirements Specifications [DEL-02].

Contractor will comply with the proposer test requirements of this Subtask 7.3 – Conduct Final Acceptance Test.

As defined within this Subtask 7.3 – Conduct Final Acceptance Test, Contractor acknowledges that upon successful completion of Subtask 4.3 – Conduct User Acceptance Test through Subtask 7.2 – Continuity of Operations Planning, County will conduct a Final Acceptance Review (FAR) to determine whether Contractor has satisfied the terms and conditions of this SOW and whether to accept the System for operational use. Upon conducting Final AT, the System will have been in productive use and well established.

During Final AT, a review shall be made of any previously submitted problem reports and verification made of closure. Any anomalies or issues discovered during UAT will be verified to have been addressed. A documentation review will be conducted, ensuring that any changes or updates have been properly annotated for future reference. Upon completion of the Final AT, County’s Project Director and Contractor’s Project Director will acknowledge completion of the implementation with a Certificate of Final Acceptance.

APPLICABLE STANDARDS

The TEMP (DEL-04) shall be adhered to for SAT and UAT.

DELIVERABLE 7.3 – FINAL ACCEPTANCE

Contractor shall provide in accordance with Subtask 7.3 – Conduct Final Acceptance Test the following Deliverable(s) for this component of the SOW:

- **DEL-29:** Configuration Management Plan.

**AGREEMENT
FOR
MBIS SOLUTION**



EXHIBIT A
STATEMENT OF WORK

DECEMBER 2014

TABLE OF CONTENTS

SECTION 3	SYSTEM OPERATION.....	1
Section 3.1	Scope of Services.....	1
Section 3.1.1	Matching.....	2
Section 3.1.2	National and International Interfaces	10
Section 3.1.3	State System Interfaces	12
Section 3.1.4	Repository Management	19
Section 3.1.5	Report Generation.....	25
Section 3.2	Support Services	29
Section 3.2.1	Scope of Support.....	29
Section 3.2.2	Customer Support	36
Section 3.2.3	Service Level Performance	37
Section 3.2.4	Training	39
Section 3.3	Program Management.....	41
Section 3.3.1	Program Organization	41
Section 3.3.2	Management and Technical Reporting and Reviews	47
Section 3.3.3	Facility Personnel	50
Section 3.3.4	System Security	51
Section 3.4	Maintenance Services	53
Section 3.4.1	Technology Refresh and Enhancements	60
Section 3.4.2	Software Updates.....	64
Section 3.4.3	System Environment	65
Section 3.4.4	Scheduled Downtime and Preventive Maintenance	65
Section 3.4.5	Response Time Monitoring	66
Section 3.5	Correction of Deficiencies.....	66
Section 3.5.1	Identification of Deficiencies.....	67
Section 3.5.2	Deficiency Priority Levels	67
Section 3.5.3	Problem Resolution and Protocols.....	68
Section 3.6	Configuration Management	68
Section 3.7	Continuity of Operations	72
SECTION 4	REMEDIES	74
Section 4.1	Service Credits	74
Section 4.2	System Response Time Deficiencies	75
ATTACHMENT A.1	– SYSTEM REQUIREMENTS	77
ATTACHMENT A.2	– PROJECT DELIVERABLES	78
ATTACHMENT A.3	– PERFORMANCE REQUIREMENTS	82
SECTION 1	STORAGE CAPACITY REQUIREMENTS	82
Section 1.1	Annual System Matrix.....	82

Section 1.2	Current LACRIS Record Counts	82
SECTION 2	SYSTEM PERFORMANCE REQUIREMENTS	83
Section 2.1	Annual LACRIS Transaction Counts	83
SECTION 3	RESPONSE TIME REQUIREMENTS.....	84
Section 3.1	Response Times per Transaction Type.....	84
SECTION 4	ACCURACY REQUIREMENTS	85
Section 4.1	Accuracy Rates by Transaction Type.....	85
SECTION 5	ACCURACY VERIFICATION REQUIREMENTS AND MEASURES	86
Section 5.1	Lights Out Accuracy Verification Conditions.....	86
Section 5.2	Best Practices Verification Conditions	86
SECTION 6	SERVICE AVAILABILITY AND RESTORATION REQUIREMENTS	87
SECTION 7	SYSTEM MAINTENANCE REQUIREMENTS	87
Section 7.1	Preventive Maintenance	88
Section 7.2	Corrective Maintenance	88
Section 7.3	Protocols	88
ATTACHMENT A.4	– SYSTEM CONFIGURATION	90
ATTACHMENT A.5	– EXISTING SYSTEM REPORT	91

STATEMENT OF WORK

SECTION 3 SYSTEM OPERATION

This section of the SOW, together with Attachment A.1 – System Requirements, Attachment A.3 – Performance Requirements and Attachment A.5 – Existing System Report, provides a detailed description of the scope of Work to be performed by Contractor throughout the operational and support phase (System Operation) of the Agreement as part of the Service Level Requirements (SLRs). Contractor shall submit to County for approval a Service Level Plan (“SLP”), based on its Service Level Proposal, which shall satisfy all Service Level Requirements specified in Section 3 – System Operation of the SOW, including this Section 3.1 – Scope of Services as well as in Attachment A.3 – Performance Requirements to the SOW and Exhibit D (Service Level Requirements).

SECTION 3.1 SCOPE OF SERVICES

Contractor shall provide for County’s Primary Site, COOP Site and Remote Sites a suite of Services that will satisfy the Service Level Requirements based on the SLP developed by Contractor. Contractor shall provide all facilities, equipment, software and personnel required to deliver the Services identified in this Section 3.1 – Scope of Services and to satisfy the SLRs for County’s Primary Site, COOP Site and Remote Sites.

The sections outline under this Section 3.1 – Scope of Services below set forth the required Services identified for the MBIS Operational Environment.

Contractor will provide the following services to fully comply with the System Operation requirements set forth in this Section 3 – System Operation of the SOW, including:

- Matching
- System Interfaces
- Repository Management
- Report Generation
- Training
- Program Organization
- Preventive and Corrective Maintenance Services

Contractor will provide all the deliverables identified in Attachment A.2 – Project Deliverables in accordance with the applicable delivery requirements.

Contractor will deliver all functionality required to satisfy the requirements of this Section 3 – System Operation of the SOW, including those set forth in Attachment A.1 – System Requirements and Attachment A.3 – Performance Requirements.

Contractor will provide all personnel, facilities, equipment, material, supplies, support, and management to satisfy these requirements. Contractor is compliant with the referenced documents listed in Section 1.3.2 – Specifications, Standards and Guides of the SOW and will

perform the steps in Section 1.3.1 – Compliance Documents of the SOW before substituting newer referenced documents.

All work under the MBIS contract will be performed within the territory of the United States and by US citizens or lawful permanent residents, unless prior written permission is obtained from the County. No County data will be stored, accessed from, or transmitted outside the US, and no County data or information will be communicated to anyone who is not a US citizen or lawful permanent resident unless prior written permission is obtained from the County.

The following sections describe the provided services in detail, including service level commitments, assumptions, risks, and applicable standards.

SECTION 3.1.1 MATCHING

Contractor shall supply friction ridge matching (known and unknown finger and palm friction ridges) as well as Iris and Facial images when transactions are submitted using ANSI/NIST compliant transactions that conform to EBTS.

Contractor will comply with the matching requirements of this Section 3.1.1 – Matching.

This section describes Contractor's approach to satisfying the matching requirements, the matching services to be provided, the capacities and response times to be supported (average and peak hour), accuracies of services, and any assumptions, risks, or constraints.

APPROACH

Contractor will supply its industry cutting edge matching algorithms, incorporating friction ridge matching for fingerprints and palmprints and fusion technology to achieve the County MBIS accuracy requirements.

The Service Level Plan (SLP, DEL-33) will be created as part of the system design process to document the repository requirements.

STORAGE CAPACITY REQUIREMENTS

MBIS storage capacities for the year 2015 and subsequent years up to year 2024, covering the initial 6-year term and the extended 4-year term, are calculated according to tables from Appendix C, section 6 of the RFP. The MBIS uses a Unified Database for MBIS information, archive repository, and transactional data. Contractor bases the sizing calculations on the number of tenprint and latent events in the System, not on the number of MAIN Numbers registered in MBIS.

MBIS ANSI/NIST ARCHIVE STORAGE CAPACITY CALCULATIONS

Contractor will comply with requirement Stor Req 1.

Table 1 provides detailed calculations for the ANSI/NIST Archive storage capacity for the years 2015-2024, assuming a 2% growth rate from 2013 levels. This storage includes demographics, images, feature templates and database indexes.

Table 1: ANSI/NIST Storage 2015-2024 (Number of Records in Thousands)

	2015	2016	2017	2018	2019
Main Subjects	4,578	4,669	4,763	4,858	4,955
Tenprint	12,485	12,734	12,989	13,249	13,514
Palm Prints	2,393	2,441	2,490	2,539	2,590
Mugshots	4,890	4,988	5,087	5,189	5,293
Unsolved Latent	260	265	271	276	282
Unsolved Latent Palm	100	102	104	106	108
Responses – Average 3 per Tenprint and MID transaction	2,194	2,238	2,283	2,329	2,375
Documents – Average 2 per Arrest and LCMS entry	1,650	1,683	1,717	1,751	1,786

Table 1 (continued)

	2020	2021	2022	2023	2024
Main Subjects	5,054	5,155	5,258	5,364	5,471
Tenprint	13,784	14,060	14,341	14,628	14,920
Palm Prints	2,642	2,695	2,749	2,804	2,860
Mugshots	5,399	5,507	5,617	5,729	5,844
Unsolved Latent	287	293	299	305	311
Unsolved Latent Palm	110	112	115	117	119
Responses – Average 3 per Tenprint and MID transaction	2,423	2,471	2,520	2,571	2,622
Documents – Average 2 per Arrest and LCMS entry	1,822	1,858	1,895	1,933	1,972

Table 2: UDB Storage 2015-2024 (In GB)

	2015	2016	2017	2018	2019
Tenprints – 500ppi, 0.72 MB	1,756	1,791	1,827	1,863	1,900
Tenprints – 1000ppi, 4.72MB	46,038	46,958	47,898	48,856	49,833

	2015	2016	2017	2018	2019
Palm Prints– 500ppi, 2.3MB	1,075	1,096	1,118	1,141	1,164
Palm Prints – 1000ppi, 13.6MB	25,425	25,933	26,452	26,981	27,521
Mugshots	239	244	248	253	258
Unsolved Latent – 0.25MB	64	65	66	67	69
Unsolved Latent Palm 0.25MB	24	25	25	26	26
Responses – Average 3 per Tenprint and MID transaction, 0.02MB	4	4	4	5	5
Documents – Average 2 per Arrest and LCMS entry 0.05MB	81	82	84	86	87
Work in Progress Queue (JOBQ) with 30 day retention (TB)	2.10	2.14	2.18	2.23	2.27
Audit Trail 5 year cumulative (TB)	0.35	0.47	0.59	0.61	0.62
Total with 20% safety factor (TB)	90.49	92.45	94.43	96.31	98.23

Table 2 (continued)

	2020	2021	2022	2023	2024
Tenprints – 500ppi, 0.72 MB	1,938	1,977	2,017	2,057	2,098
Tenprints – 1000ppi, 4.72MB	50,829	51,846	52,883	53,941	55,019
Palm Prints – 500ppi, 2.3MB	1,187	1,211	1,235	1,259	1,285
Palm Prints – 1000ppi, 13.6MB	28,071	28,632	29,205	29,789	30,385
Mugshots	264	269	274	280	285
Unsolved Latent 0.25MB	70	72	73	74	76
Unsolved Latent Palm 0.25MB	27	27	28	29	29
Responses Average 3 per Tenprint and MID transaction, 0.02MB	5	5	5	5	5
Documents Average 2 per Arrest and LCMS entry 0.05MB	89	91	93	94	96
Work in Progress Queue (JOBQ) with 30 day retention (TB)	2.32	2.36	2.41	2.46	87

	2020	2021	2022	2023	2024
Audit Trail 5 year cumulative (TB)	0.63	0.64	0.66	0.67	0.68
Total with 20% safety factor (TB)	100.21	102.20	104.26	106.33	108.47

Contractor will comply with **Stor Req 4** by providing an LTO-5 tape backup system and COTS backup management software.

Contractor will comply with requirement **Stor Req 5** for MBIS-logged storage capacity. The compressed logs will occupy approximately 150 GB of disk space. MBIS will have the capacity and ability to create and store MBIS level logs for all activities listed in the Functional Requirements for a period commensurate with the FBI CJIS Security Policy, version 5.2, plus 3 additional years.

MBIS FEATURE SETS CALCULATIONS

Contractor will comply with **Stor Req 2** and **Stor Req 3**. Contractor calculates that the template database will total 1.2 TB in 2024.

The template database contains:

- One 20 finger composite record for tenprint searches
- Three 20 finger event records with 2 templates each for latent fusion searches
- One two-hand upper, lower or full, and writers palm for palm latent searches
- Unsolved latent finger with 2 templates each for latent fusion searches
- Unsolved latent palm
- Face templates

Table 3: Template Storage for 2024

	2024 COUNT	TEMPLATE SIZE (B)	STORAGE (MB)
20 Finger Tenprint	5,471,000	23,476	122,484
20 Finger Latent	14,921,000	56,000	796,840
Known Palm	2,860,000	150,000	409,092
Unsolved Latent Finger	311,000	2,000	560
Unsolved Latent Palm	120,000	1,000	114
Face	5,844,000	2,531	14,106
Total (2 copies stored for redundancy)			3,174 GB
Total MU Capacity	32 MU	113GB memory available	3,616 GB

THROUGHPUT AND RESPONSE TIMES

Contractor will comply with requirement **ThruPut Req 1** through **4** and **Response Req 1** and **2**. The proposed System provides the matching resources needed to satisfy throughput requirements for the contract years up through 2024 based on the hourly transaction rate and response time shown in

Table 5. Ninety-five percent of transactions will meet the required response time as measured from ingest through response, excluding operator intervention and delays caused by interfacing to other CJIS systems and network.

Contractor acknowledges that the MBIS throughput rates will grow over the life of the System based on Section 2.1 (Annual LACRIS Transaction Counts) of Exhibit 2 (Performance Requirements) to Appendix B (Statement of Work) to the RFP. Table 4 projects the growth for the Existing System agreement.

Table 4: Annual LACRIS Transaction Counts (2015 – 2024)

	2015	2016	2017	2018	2019
CRM	347,224	354,169	361,252	368,477	375,847
CUS	0	0	0	0	0
REG	9,381	9,569	9,760	9,955	10,154
SUP	0	0	0	0	0
COR	0	0	0	0	0
IDN	13,420	13,688	13,962	14,241	14,526
IDN2	0	0	0	0	0
IDN4	452,046	497,251	546,976	601,673	661,841
APP	0	0	0	0	0
Latent	62,332	63,579	64,850	66,147	67,470
Palm Latent	30,799	31,415	32,044	32,685	33,338
TLI	366,242	373,567	381,038	388,659	396,432
CRM	383,363	391,031	398,851	406,828	414,965
CUS	0	0	0	0	0
REG	10,357	10,565	10,776	10,991	11,211
SUP	0	0	0	0	0
COR	0	0	0	0	0
IDN	14,817	15,113	15,415	15,724	16,038
IDN2	0	0	0	0	0
IDN4	728,025	800,827	880,910	969,001	1,065,901

	2015	2016	2017	2018	2019
APP	0	0	0	0	0
Latent	68,820	70,196	71,600	73,032	74,493
Palm Latent	34,005	34,685	35,379	36,086	36,808
TLI	404,361	412,448	420,697	429,111	437,693

Response times are based on transactions being evenly spaced throughout the peak hour. The MBIS can sustain the peak hourly workload for 10 hours. The proposed System shall use transaction priority management that processes higher-priority transactions ahead of lower-priority transactions in the same transaction class when the transaction rate exceeds the peak design level.

Table 5: Peak Hour Transaction Counts 2015-2024

	2015	2016	2017	2018	2019
Tenprint TP-TP	101	104	106	108	110
Tenprint/Latent TP-LT	101	104	106	108	110
Tenprint/Palm Latent KP-LT	13	13	14	14	14
Latent LT-TP	34	35	36	36	37
Palm Latent LT-KP	17	17	18	18	19
Mobile ID TP-TP	99	101	103	105	107
Face to Face	54	55	56	57	58
Tenprint TP-TP	112	114	117	119	121
Tenprint/Latent TP-LT	112	114	117	119	121
Tenprint/Palm Latent KP-LT	14	15	15	15	16
Latent LT-TP	38	39	39	40	41
Palm Latent LT-KP	19	19	20	20	20
Mobile ID TP-TP	109	111	114	116	118
Face to Face	59	60	62	63	64

Table 6: Response Time Per Transaction Type

TRANSACTION CLASS TYPES	RESPONSE REQUIREMENTS UNDER PEAK LOAD	OPERATIONAL HOURS
Criminal TP-TP	1 minute	24 Hour
Tenprint/Latent TP-LT	1 minute	24 Hour

TRANSACTION CLASS TYPES	RESPONSE REQUIREMENTS UNDER PEAK LOAD	OPERATIONAL HOURS
Latent LT-TP	1 minute	24 Hour
Palm LT-KP	10 minutes	24 Hour
Criminal KP-LT	5 minutes	24 Hour
Mobile ID TP-TP	30 seconds	24 Hour
Face to Face	1 Minute	24 Hour

ACCURACY

Contractor will comply with requirement **Accuracy Req 1**, summarized in the following three tables. The accuracy is greatly affected by repository quality and transaction image quality. Table 7 depicts the requirements for best practice processing.

Table 7: Best Practices Accuracy Verification Conditions

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Search Records	10,000	10,000	200	5,000	100
Mated Records	50%	100	100	10	40
NFIQ Average of Mated TPs	1	1	1	N/A	N/A
Minimum Number of Simultaneous Minutiae of Mated Items	N/A	12	12	12	12
Selectivity	1	10/25	10/25	10/25	10/25
True Match Rate	99.9%	93% / 100%	93% / 100%	93% / 100%	93% / 100%
Non-Mated Search Records	50%	9,900	100	4,990	60
Background Repository	All Converted TP Records	All Converted LT Records	All Converted TP Records	All Converted Palm LT Records	All Converted KP Records

Contractor shall comply with the selectivity and true match rates as identified in the tables above. To achieve the 100% match rate, Contractor will use all of its technology and multi-stage match processes. In a dynamic field such as biometric identification, achieving 100% on any test has inherent limitations and risks. Contractor would respectfully request the following considerations to meet this requirement:

- More than one latent examiner will be allowed to process the latent due to differences in manual encoding.
- Extremely poor-quality latents and mated tenprints will be excluded from the test set.
- All latents must have a minimum of 16 minutiae points.

LEVELS OF SERVICE

MBIS will provide the transaction throughput level and response time in Table 5 and Table 6. It will also provide the repository sizing shown in Table 2.

Please refer to the Service Level Proposal (SLP, **DEL-33**).

ASSUMPTIONS

Contractor assumes:

- The number of records and average size of each record stated and
- Table 2 are correct.
- In the event the peak hour transaction count in
- Table 5 is exceeded for a period of time, the response time commitment will be relaxed proportionately for that period of time.
- Repository and probe images meet the requirements in for the accuracy testing.
- The design is based on a 2% growth rate, per requirement.
- Throughput and response time calculations are based on an average of 12 minutia points and an AMR of 50%.

RISKS

Table 8 lists the risks and mitigation strategies for meeting the accuracy requirements.

Table 8: Matching Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Poor legacy database quality	Contractor will have multiple events (including migrating the legacy data) of the record in the MBIS database, employ multiple matching algorithms and multi-stage matching processes, including template and score fusion.
Variance in latent examiner encoding	Contractor will provide extensive best practice training to enhance latent examiners' expertise.

APPLICABLE STANDARDS

- California Department of Justice (Cal-DOJ) Live Scan Transmission Standards
- Electronic Biometric Transmission Specification (EBTS), NGI-DOC-01078-10.0.
- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.

- IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverable(s):

- **DEL-33:** Service Level Plan

SECTION 3.1.2 NATIONAL AND INTERNATIONAL INTERFACES

Contractor shall maintain Interfaces with state and national services through the Wide Area Network (WAN) using FBI EBTS and CalDOJ conformant transactions and international transactions via the CJIS gateway.

Contractor will comply with the system interface requirements of this Section 3.1.2 – National and International Interfaces.

This section describes Contractor's approach to satisfying the system interface requirements. It identifies the interfaces with criminal repositories and other relevant law enforcement systems, applicable interface standards, any limitations in our implementation of those standards, interface capacities (average and peak hour), and any assumptions, risks, or constraints.

APPROACH

The key interfaces/exchanges operational and required in the LACRIS environment are described in the below.

The communications interface tier provides standards-based communication interface protocols. LASD MBIS will open industry standard protocols to interface with the external systems. By supporting multiple legacy and latest communication protocols, this layer enables interoperability between SOA components that are internal and external to the iESB server.

Table 9: FBI-IAFIS Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	FBI-IAFIS – IAFIS is operated and managed by the FBI. Currently, tenprint transactions are automatically forwarded to FBI IAFIS by CAL-ID.

ENTITY	DESCRIPTION
Exchange Data Type/Protocols	<p>Data includes fingerprint, palmprint, latent and mugshot data (iris and voice in future) and NIST/EBTS compliant.</p> <p>Transactions will be sent to CalDOJ which in turn will get forwarded to FBI-IAFIS.</p> <p>FBI-IAFIS responses will be received at CalDOJ and will be forwarded to LASD MBIS through the CLETS drop printers (current implementation). In future, this will change to the NIST/EBTS formatted data using electronic interface.</p>
Proposed communication Protocol options (Supported)	<p>REQUEST – SFTP/FTP/ SMTP/Web Services through state WAN.</p> <p>RESPONSE – SFTP/FTP/ SMTP/Web Services through state WAN.</p>
Interface methodology and data exchange details	<p>The NIST/EBTS tenprint requests for tenprint, latent, image retrieval, FID (Future), IID (Future) will be sent to CalDOJ AFIS first and will be forwarded by CalDOJ to FBI-IAFIS for the FBI processing. The Type 2 fields will be adjusted and validated at the post process stage in order to comply with DOJ and FBI-IAFIS specific requirements.</p> <p>The responses received from FBI-IAFIS (compliant with NIST/EBTS) by CalDOJ will be forwarded to the MBIS. At LASD MBIS, the response files will be read to identify the FBI IAFIS induced Type 1 and 2 fields.</p>
Existing capability	<p>Such interfaces are in place on current Contractor installations in California (for example, San Bernardino / Riverside County AFIS).</p> <p>Direct FBI-IAFIS system interfaces are in place at all the remote Contractor AFIS installations. A few examples include:</p> <ul style="list-style-type: none"> • WIN MBIS • Pennsylvania AFIS • Virginia AFIS • Illinois State AFIS • Georgia Bureau of Investigation

LEVELS OF SERVICE

The turnaround time for transactions that pass between the MBIS and the external systems listed above (acknowledgements, searches, responses, error notifications, updates, downloads (e.g., crime code, Live-Scan tables, validations tables, etc.), administrative messages, bulk downloads, bulk updates, etc.) for each of the interfaces will have to be identified and documented.

These will be discussed during the post contract, interface design discussion meetings.

ASSUMPTIONS

1. Each of the above stated interfaces has been tested during the SAT and UAT.

2. The required network infrastructure is in place and the appropriate ports have been identified and are enabled in support of the above stated interfaces.
3. Each of the above stated interfaces has been tested in the production environment during pre-production testing.

RISKS

Table 10: System Interfaces Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Interface to Cogent "Tickler table" for updates to the Los Angeles County PhotoManager system based on proprietary protocols.	Conduct detailed technical discussions with LASD team to understand the requirements of this interface. If required Contractor will work towards creating an API façade which will help in seamless integration with the PhotoManager.

APPLICABLE STANDARDS

- o W3C standards
- o Web Services standards methodology
- o FTP/SMTP/SFTP protocol methodology – Implementation best practices
- o CJIS Security
- o NIST / EBTS
- o California DOJ Type 2 (Adaption of the EFTS/EBTS)

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- o Interface services for the above stated interfaces. These will be hosted in the Contractor iESB.
- o **DEL-33: Service Level Plan.**

SECTION 3.1.3 STATE SYSTEM INTERFACES

Contractor shall maintain Interfaces with all requisite data repositories and systems and with networks that in turn connect to booking stations and other criminal justice systems using the FBI EBTS. These Interfaces, required for the successful implementation of the System during Phase 1 of this SOW, are documented in the Existing System Report (Attachment A.5 – Existing System Report).

Contractor will comply with the system interface requirements of Section 3.1.3 – State System Interfaces of the SOW.

This section describes Contractor's approach to satisfying the system interface requirements. It identifies the interfaces with criminal repositories and other relevant law enforcement systems, applicable interface standards, any limitations in our implementation of those standards, interface capacities (average and peak hour), and any assumptions, risks, or constraints.

APPROACH

The key interfaces/exchanges operational and required in the LACRIS environment are described in the Table 11.

The communications interface tier provides standards-based communication interface protocols. LASD MBIS will open industry standard protocols to interface with the external systems. By supporting multiple legacy and latest communication protocols, this layer enables interoperability between SOA components that are internal and external to the iESB server.

Table 11: CAL-DOJ AFIS Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	CalDOJ Automated Fingerprint Identification System (AFIS) – The California Identification System (CAL-ID) is the AFIS managed by the CALDOJ. LAFIS forwards all fingerprint transactions to CAL_ID by FTP and Web Services, after local processing is complete.
Exchange Data Type/Protocols	Includes fingerprint, palmprint, latent and mugshot data (iris and voice in future). NIST/EBTS. Search transactions will be sent to CalDOJ. CalDOJ Responses will be received at the CLETS drop printers (current implementation). In future this will change to the NIST/EBTS formatted data using electronic interface.
Proposed communication Protocol options (Supported)	REQUEST – SFTP/FTP/ SMTP/Web Services through State WAN RESPONSE – SFTP/FTP/ SMTP/Web Services through State WAN
Interface methodology and data exchange details	The NIST/EBTS tenprint requests for tenprint, latent, image retrieval, FID (Future), IID (Future) will be sent to CalDOJ AFIS for processing. The Type 2 fields will be adjusted and validated at the post-processing stage in order to ensure they comply with CalDOJ specific requirements. The responses received from CalDOJ (if available in electronic form, compliant with NIST/EBTS) will be received by the MBIS. At the MBIS, the response files will be read to identify the State induced Type 1 and 2 fields.
Existing capability	Such interfaces are in place on current Contractor ABIS installation in California (for example, San Bernardino / Riverside County AFIS).

Table 12: County Live-Scan Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	County Live-Scan System – The County’s Live-Scan system is the tenprint data source (initial input devices) for LAFIS. Live-Scan communicates with LAFIS by FTP. LAFIS communicates with Live-Scan by e-mail.
Exchange Data Type/Protocols	Data includes fingerprint, palmprint and mugshot data and NIST/EBTS compliant. Search TOT will be received from the Live-Scan and the responses (local processing, CalDOJ responses, FBI-IAFIS responses) will be forwarded to the County Live-Scans.
Proposed communication Protocol options (Supported)	REQUEST – SFTP/FTP through State WAN RESPONSE – SMTP/FTP through State WAN Future Web Service Support
Interface methodology and data exchange details	The Live-Scan will send the search transactions to MBIS (NIST/EBTS) and the same will be processed at the MBIS. As necessary, the transactions will be forwarded to CalDOJ and FBI/IAFIS. The responses (NIST/EBTS) for the local MBIS (Error/Normal responses) will be sent to the Live-Scans through this interface. The CalDOJ and FBI-IAFIS responses (Error/Normal responses), if available in (NIST/EBTS) format will be forwarded by the MBIS to the Live-Scans through this interface.
Existing capability	Such interfaces are in place on current Contractor installations in California (for example, San Bernardino / Riverside County AFIS). Live-Scans system interfaces are in place at all the Contractor AFIS installations. A few examples include: <ul style="list-style-type: none"> • WIN MBIS • Pennsylvania AFIS • Virginia AFIS • Illinois State AFIS

Table 13: County Warrant System Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	County Warrant System (CWS) – LAFIS has the ability to communicate with Los Angeles County’s CWS through the County’s Justice Data Interface Controller (JDIC) using TCP/IP.
Exchange Data Type / Protocols	Tenprint (NIST/EBTS)

ENTITY	DESCRIPTION
Proposed communication Protocol options (Supported)	Request and Response option supported - TCP/IP socket communication via MBIS Intranet/JDIC.
Interface methodology and data exchange details	The proposed MBIS will interface with CWS via the County's Justice Data Interface Controller (JDIC), as it happens in current environment, and send the necessary data.
Existing capability	Contractor has a proven experience in interfacing with local agency level CCH systems as well as County level RMS/JMS and mugshot systems. Almost all Contractor installations support external CJIS system interfaces that are built custom to the site, but which use the open standard methodology and programming languages.

Table 14: County AJIS Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	County Automated Justice Automated System (AJIS) – AJIS maintains arrest, booking, and custody information for offenders in Los Angeles County. Currently, AJIS receives its positive fingerprint-based identifier (MAIN #) from the LAFIS.
Exchange Data Type / Protocols	Tenprint (NIST/EBTS)
Proposed communication Protocol options (Supported)	Request and Response option supported - TCP/IP over MBIS Intranet (LA County Secure Network)
Interface methodology and data exchange details	The proposed MBIS will continue to interface with AJIS as it happens in current environment and send MAIN # based on the positive identification at the MBIS.
Existing capability	Contractor has a proven experience in interfacing with state level CCH systems as well as County level RMS/JMS and mugshot systems. Almost all Contractor installations support external CJIS system interfaces that are built custom to the site, but which use the open standard methodology and programming languages.

Table 15: County Mugshot System Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	County Mugshot System – Los Angeles County Photo Manager (LAPM) is the county repository for mugshot images. LAFIS supplies LAPM with positive ID matches against the LAFIS database through FTP and tickler table.
Exchange Data Type / Protocols	Tenprint (NIST/EBTS)
Proposed communication Protocol options (Supported)	Request and Response option supported - FTP/Tickler table queries
Interface methodology and data exchange details	The proposed MBIS will continue to interface with LAPM as it happens in current environment and send MAIN # based on the positive identification at the MBIS.
Existing capability	Contractor has a proven experience in interfacing with state level CCH systems as well as county level RMS/JMS and mugshot systems. Almost all Contractor installations support external CJIS system interfaces that are built custom to the site, but which use the open standard methodology and programming languages.

Table 16: Mobile ID Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	Mobile ID – This allows access by mobile identification devices to LAFIS from the field, for the submission of inquiries, and the return of responses. Transactions are managed through the Proposer's proprietary Web page.
Exchange Data Type / Protocols	Tenprint (NIST/EBTS)
Proposed communication Protocol options (Supported)	Request and Response option supported – Web Services/ Web Interface/SMTP

ENTITY	DESCRIPTION
Interface methodology and data exchange details	<p>The MBIS will communicate with the Mobile ID devices through e-mail/web service interfaces.</p> <p>The Mobile ID devices will send the search transactions to MBIS (NIST/EBTS) and the same will be processed at the MBIS.</p> <p>As necessary the transactions will be forwarded to CalDOJ and FBI/IAFIS.</p> <p>The responses (NIST/EBTS) for the local MBIS (Error/Normal responses) will be sent to the Mobile ID devices through this interface.</p> <p>The CalDOJ and FBI-IAFIS responses (Error/Normal responses), if available in NIST/EBTS format, will be forwarded by the MBIS to the Mobile ID devices through this interface.</p>
Existing Capability	California Department of Justice, Western Identification Network, Illinois State Police, Michigan State Police, Virginia State Police.

Table 17: Field Latent Capturing Devices Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	Field Latent Capturing Devices (Optional) – This interface allows access to Field Latent Capturing Devices for the mobile investigation and latent registration to MBIS from the field, for the submission of inquiries, and the return of responses.
Exchange Data Type / Protocols	Latent and Tenprint (NIST/EBTS)
Proposed communication Protocol options (Supported)	Request and Response option supported – Web Services/ Web Interface/SMTP
Interface methodology and data exchange details	<p>The MBIS will communicate with the Field Latent Capturing Devices through e-mail/web service interfaces.</p> <p>The Field Latent Capturing Devices will send the Latent search transactions to MBIS (NIST/EBTS) and the same will be processed at the MBIS.</p> <p>As necessary the transactions will be forwarded to CalDOJ and FBI/IAFIS.</p> <p>The responses (NIST/EBTS) for the local MBIS (Error/Normal responses) will be sent to the Field Latent Capturing Devices through this interface.</p> <p>The CalDOJ and FBI-IAFIS responses (Error/Normal responses), if available in NIST/EBTS format, will be forwarded by the MBIS to the Field Latent Capturing Devices through this interface</p>

Table 18: Iris Devices Interface Requirements

ENTITY	DESCRIPTION
Interface Requirement	Iris Devices (Future).
Exchange Data Type / Protocols	Iris Transactions as per NIST/EBTS. Search TOT transactions will be received from the Iris Devices and the responses (Local processing, CalDOJ responses, FBI-IAFIS responses) will be forwarded to the Iris device management server.
Proposed communication Protocol options (Supported)	REQUEST option supported = SFTP/FTP through State WAN RESPONSE option supported= SMTP/FTP through State WAN Future Web Service Support
Interface methodology and data exchange details	The Iris Devices will send the search transactions to MBIS (NIST/EBTS) and the same will be processed at the MBIS. As necessary the transactions will be forwarded to CalDOJ and FBI/IAFIS. The responses (NIST/EBTS) for the local MBIS (Error/Normal responses) will be sent to the Iris Devices through this interface. The CalDOJ and FBI-IAFIS responses (Error/Normal responses), if available in (NIST/EBTS) format will be forwarded by the MBIS to the Iris device management server through this interface.

LEVELS OF SERVICE

The turnaround time for transactions that pass between the MBIS and the external systems listed above (acknowledgements, searches, responses, error notifications, updates, downloads (e.g., crime code, Live-Scan tables, validations tables, etc.), administrative messages, bulk downloads, bulk updates, etc.) for each of the interfaces will have to be identified and documented.

These will be discussed and mutually agreed upon during the post Agreement, interface design discussion meetings.

ASSUMPTIONS

1. Each of the above stated interfaces has been tested during the SAT and UAT.
2. The required network infrastructure is in place and the appropriate ports have been identified and are enabled in support of the above stated interfaces.
3. Each of the above stated interfaces has been tested in the production environment during pre-production testing.

RISKS

Table 19: System Interfaces Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Interface to Cogent "Tickler table" for updates to the Los Angeles County PhotoManager system based on proprietary protocols.	Conduct detailed technical discussions with LASD team to understand the requirements of this interface. If required Contractor will work towards creating an API façade which will help in seamless integration with the PhotoManager.

APPLICABLE STANDARDS

- W3C standards
- Web Services standards methodology
- FTP/SMTP/SFTP protocol methodology – Implementation best practices
- CJIS Security
- NIST / EBTS
- California DOJ Type 2 (Adaption of the EFTS/EBTS)

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- Interface services for the above stated interfaces. These will be hosted in the Contractor iESB.
- **DEL-33: Service Level Plan.**

SECTION 3.1.4 REPOSITORY MANAGEMENT

Contractor shall maintain access to a well-maintained and indexed repository of all enrolled transactions, stored and retrievable in FBI EBTS formats. The ability to update, delete, retrieve and print appropriate card formats and other forms or link enrolled transactions, shall be provided.

Contractor will comply with the repository management requirements of Section 3.1.4 – Repository Management of the SOW.

This section describes Contractor's approach to satisfying the repository management requirements, the procedures for maintaining the repository and for ensuring the integrity, confidentiality, and accessibility of the contents.

APPROACH

The MBIS repository solution is a well maintained and indexed repository that provides authorized users the ability to retrieve, update, delete, consolidate, and print appropriate repository records and transaction records in FBI or County EBTS formats. Authorized

users can print card formats and other documents as well as link enrolled transactions as required and is detailed below. Contractor fully complies with the requirements for repository management set forth in Section 3.1.4 – Repository Management of the SOW. SLP (DEL-33) will be created as part of the system design process to document the repository requirements

Details of our procedures for maintaining the repository and for ensuring the integrity, confidentiality and accessibility of the contents are provided in this section.

The MBIS data repository consists of three databases: Unified Database, containing the ANSI/NIST data and feature data; Transaction Database, containing all transactional information for the work in progress; and Audit and reporting, containing all audit trail and used for reports.

ACCESSIBILITY

The MBIS will provide a role based security model. The System will be predefined with a set of functions that can be assigned to individual users or groups. Individual functions will then be used to control user access to both application features and repository data. System Data access functions will determine whether a user has the access to view or change restricted data, for example, sealed records. Users without the functions to access restricted data will be unaware that the data exists on the System. The security model will also provide for the concept of groups. Each group in the System can have individual System functions associated with it. Users can then be added to these groups which will make the same System functions available to multiple users without having to assign the functions at an individual user level. System logins and passwords will be governed by CJIS security requirements (for example, strong passwords adhering to complex rules including use of special characters, must change every 90 days, and unique user IDs). Figure 1 depicts the assignment of user privileges through the web interface.

Figure 1: User Management

The screenshot displays the 'Save User' interface within the NEC Integrated System Monitoring application. The form includes the following fields and sections:

- User Information:** User ID (A0000), System ID (U7), User Name (Administrator), Start Date (12/18/2009), End Date (12/18/2020), Authentication Type (Database Authentication), System Account (A7), Email Address (administrator@default.com), Contact Number, Department/Organization, Change Password On Next Login (checked), Password, Confirm Password, and Certificate Name.
- Roles:** A section with a list of roles and checkboxes for selection. The roles listed are: All TOT, U7W User, System Administrator, Access Control for ESW Users, FAT Testprint, ESW WebServices, ALL TOT, and CAR_Criminal Arrest Record.
- Domains:** A section with a list of domains and checkboxes for selection. The domains listed are: PRODUCTION, TEST, and TRAINING.
- Default Domain:** A dropdown menu set to PRODUCTION.
- Password:** Fields for Password and Confirm Password.
- Buttons:** A 'Reset' button and a 'Save' button.
- Footer:** Created By: SYSTEM, Created Date: 12/18/2009 00:00:00, Last Updated By: U7ADMIN, Last Updated Date: 07/17/2013 09:33:15.

- **Confidentiality** – The MBIS ANSI/NIST storage is logically separated into segments based on data security requirements, with view and update privileges to the segments based on user profile. The data confidentiality is controlled by access levels set for each group of users and can be set to allow view only, allow view and update, or not allow any access. The user profile also contains actions permitted for operators or groups of operators. All actions are logged into the audit trail by action performed, user ID and date/time.

In addition, no County data will be stored, accessed from or transmitted to any agency, inside or outside the United States, without permission from the county. No County data or information will be communicated to anyone who is not a US citizen or lawful permanent resident unless prior permission is obtained in writing from County.

- **Integrity** – To maintain the integrity of the repository, Contractor has selected industry standard Oracle 11g relational database and RAID 6 SAN storage. If the optional COOP System is chosen, the COOP Site will house an identical configuration. Oracle Active Data Guard synchronizes the data between the Primary Site and COOP Site in real time. Oracle Active Data Guard also enables the use of fast incremental backups when offloading backups to external media. Contractor will use LTO 5 tape library to perform data backup.
- **Maintaining** – The repository manager hosts all the MBIS data, including Archive, transaction data and iESB-specific system configuration database, and the AIM database into a single database called the Unified Database (UDB). UDB simplifies repository maintenance by providing a single point of database access, eliminating synchronization between multiple databases, offering a streamlined database backup policy, and providing a single most up-to-date view of the data to the users.

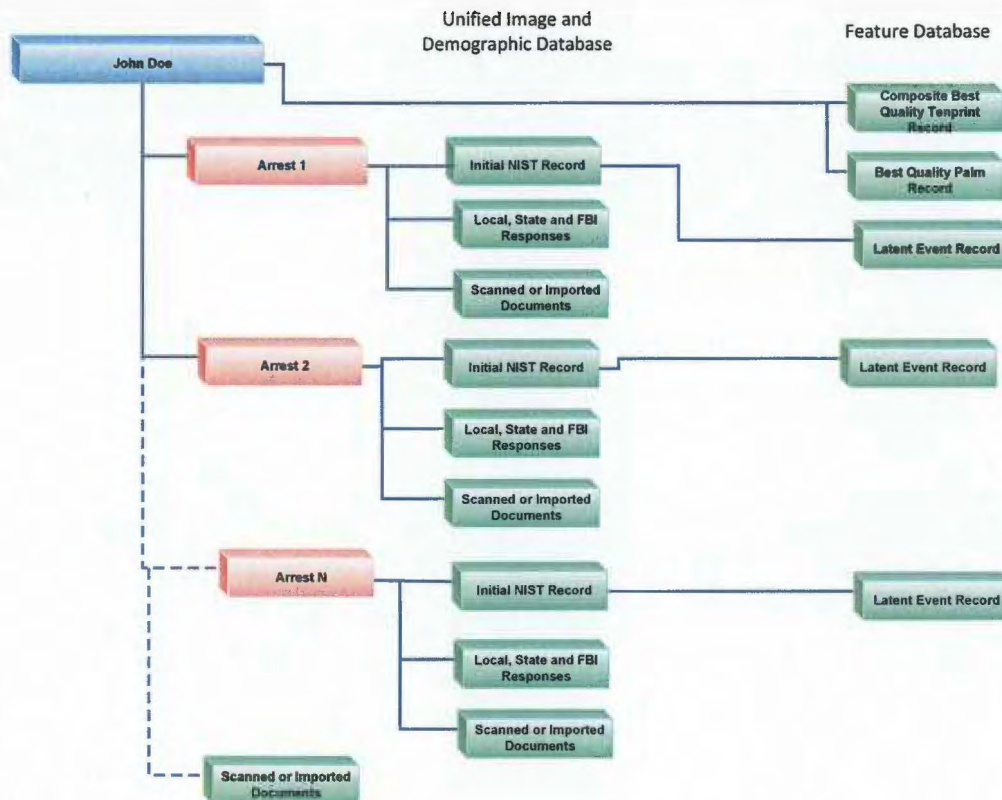
MBIS UDB FEATURE DATABASE

The Unified Image and Demographic Database (UDB) contains all the records received and is event based. This database contains all demographic and image information used in the MBIS.

The Unified Database (UDB) is broken down into two sections:

- NIST Archive UDB Image and Demographic Database
- MBIS UDB Feature Database used for matching

Figure 2: Unified Image and Demographic Database



The MBIS UDB feature database contains the information used for matching fingerprints, the fingerprint templates. It is divided into several sections for better efficiency:

- **RDB (Rolled Database) for Tenprint** – Contains all ten rolled fingerprints. It is used for searching Tenprint Inquiries (TI) and will contain the best quality images for each individual.
- **SDB (Slap Database) for Tenprint** – Contains all 10 slap fingerprints extracted from the NIST type 4 or 14 record. It is used for searching Tenprint Inquiries (TI) and will contain the best quality images for each individual.
- **RDB (Rolled Database) for Latent** – Contains all ten rolled fingerprints for up to three arrests. It is used for searching Latent Inquiries (LI).

- **SDB (Slap Database) for Latent** – Contains all 10 slap fingerprints extracted from the NIST type 4 or 14 record for up to three arrests. It is used for searching Latent Inquiries (LI).
- **LDB (Unsolved Latent Database)** – Contains unsolved latent fingerprints and is used for searching known Tenprint-to-Latent Inquiries (T/LI).
- **PDB (Palmpoint Database)** – Contains palmpoints (upper, lower, and writers' palmpoints from both hands) from each individual and is used for searching Latent Palmpoint Inquiries (LI-P).
- **LDB-P (Unsolved Latent Palmpoint Database)** – Contains unsolved latent palmpoints and is used for searching known Palmpoint-to-Latent Inquiries (T/LI-P).
- **FDB (Face Database)** – Contains face templates from each arrest and is used for latent face inquiries.
- **NIST Archive**

The NIST Archive holds the NIST records as received from submitters. It also holds supplemental documents (scanned or imported), response messages from the FBI, and photographs. These records are linked to the MBIS matching database through the unified image and demographic database.

The county will also be able to create folders which are not person specific. These will be identified by a folder ID, which can be the incident number of any format County desires. Documents can be scanned or imported and assigned to the incident.

TRANSACTION DATABASE

The MBIS transaction database keeps track of all jobs running on the MBIS. It is used and managed through the job queue. The job queue stores the transaction state information, so if a transaction is interrupted for any reason, that transaction can be reinitiated from the previous stable state. Transactions are not confined to a single workstation, allowing for collaboration and the ability to continue processing if the input workstation goes offline.

AUDIT TRAIL

The MBIS provides an audit trail capability to assist with statistical reporting and to provide an additional security measure for the data stored within the application. Before starting specific activities, MBIS records the event in the audit trail. The audit trail is updated at the beginning of each task to ensure that subsequent journal entries are created in chronological order.

For example, a user may ask MBIS to display a specific record. MBIS records that the user requested the record along with the system date and time. These events are stored in the correct chronological order. Authorized users can query the audit trail through standard and ad hoc reports.

MBIS tracks all user activity through the audit trail. Activities performed on records with special statuses are also tracked. Because of this, MBIS will filter out audit trail entries relating to users, folders, and documents that the user requesting the report is not authorized to see. This filtering may cause different MBIS users to receive different report results with the same query.

Audit data will be kept in the System for a minimum of five years or it may be retained for longer depending on system designed storage. At that time, the data will be archived using industry standard database backup software. If the data is needed, it can be restored using industry standard restoration software.

LEVELS OF SERVICE

MBIS will provide repository sizing for all records as described in Section 3.1.1 of this document,

Table 1,

Table 2 and Table 3. Service Levels are as defined in the Service Level Proposal (SLP, DEL-33).

ASSUMPTIONS

Contractor assumes EBTS records are received in an industry standard NIST/California EBTS format. This includes tenprints, latents, palmprints, mugshots and associated demographic data. Non-NIST records (documents, photographs, etc.) will be in an industry standard format.

RISKS

Table 20: Repository Management Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Database Quality	Contractor will have multiple events (including migrating the legacy data) of the record in the MBIS database, employ multiple matching algorithms and multi-stage matching processes, including template and score fusion.
Transaction Image Quality	Contractor will use image enhancement algorithms, multiple matching algorithms, template and score fusion.

APPLICABLE STANDARDS

- o American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- o Electronic Biometric Transmission Specification (EBTS), NGI-DOC-01078-10.0.
- o IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- o IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- o IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- o FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.

- California Department of Justice (Cal-DOJ) Live Scan Transmission Standards.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-33:** Service Level Plan.

SECTION 3.1.5 REPORT GENERATION

Contractor shall maintain access to County staff, the Remote Site administrators, FBI auditors and other authorized personnel to inspect the repository, the log of transactions and performance/throughput rates, and user-level access history in order to allow County to generate predefined (canned) reports as well as ad hoc reports.

Contractor will comply with the report generation requirements of Section 3.1.5 – Report Generation of the SOW.

This section describes Contractor's approach to satisfying the report generation requirements, identifies the data to be collected or made available; the frequency at which data is collected; and special circumstances under which data is collected, describes how data will be stored, accessed, queried, and how long it will be retained, procedures for ensuring data integrity. It also describes the standard reports, their contents, the frequency of reporting, the recipients (organizations) of the reports and Ad-hoc reports.

APPROACH

Contractor's administration client, Integrated System Monitoring (ISM), is a web-based application that manages all reporting services (including standard and ad-hoc) and can be accessed from any workstation by an authorized user.

Contractor will demonstrate compliance with LASD's reporting requirements by addressing the following: data (collection, storage, accessibility, retention, and integrity), standard, and ad-hoc reporting in the subsequent sections.

DATA

The Unified Database (UDB) provides a single data repository for MBIS, Archive, and transaction data. All data updates, transaction processing, and user activity is further audited in a centralized audit trail stored within the UDB. This allows Contractor to comply with the Admin Function 21 requirements relating to tracking, monitoring, and producing reports. Table 21 illustrates how the proposed MBIS captures the data to meet the County MBIS System Requirements.

Table 21: Reports Data

	CAPTURED DATA
What is collected?	Transactions processed through the County MBIS to include data selected by work flow and TOT as described in the reports requirements under Administrative Functions and Requirements.
	User activity on individual workstations including login and logout activity.
	Latent case management activity to satisfy the LCMS reporting

	CAPTURED DATA
	requirements. Database statistics including capacity, utilization, and storage sizes to meet the County requirements including data for: <ul style="list-style-type: none"> • Criminal, civil, ID slaps and/or tactical submissions • For databases, archives and matchers • Administrative reports for each County MBIS matcher
How often is it collected?	The frequency of the data collection is real time.
Where is it stored?	The data is stored in the auditing tables within the UDB database.
How is it accessed?	The data is accessed through a user friendly report generation web interface in the reporting section of the administration client (that is, via ISM).
Length of retention?	The length of retention will be compliant to CJIS requirements and shall not exceed four years.
Integrity?	The reporting data integrity matches the integrity provided to the repository itself.

STANDARD REPORTS

Contractor will provide authorized users access to inspect the repository, the transaction history, System performance, throughput rates, and user-level access history in order to generate both predefined and ad-hoc reports. Reports are available for individual agencies as well as collectively for all agencies that participate in the County MBIS. Since the data is collected in real time, the frequency of the report generation is flexible and can be controlled by the individual operator. Contractor will comply with the **Admin Function 20** requirement stipulating that all reports can be printed on any available printer configured on the client system. The reports can also be exported in Word, Excel, CSV, XML, TIF and PDF formats, which provides the operator electronic storage and ease of distribution.

All summary reports contain start and end date dimensions, defaulting to the past full month as the report date range. Users can select the start and end dates of their choice with granularity up to the second. All detailed reports are specific to a particular case number, TCN, Master County ID and/or Job ID and can be obtained for multiple months. Table 22 provides descriptions of standard reports delivered with the MBIS.

Table 22: Standard Reports

REPORT	DESCRIPTION
STANDARD USER REPORTS	
DB Count	Provides the record count, gender breakdown, and disk space consumption for each of the databases.
DB Statistics	Provides Tenprint and Latent database statistical breakdowns by Gender, Quality, Pattern, Finger Number, Minutia Count, and Year of Birth.

REPORT	DESCRIPTION
Job Log Summary Report	Accumulative activity counts such as Tenprint Inquiries, Registrations, Tenprint Deletions, Latent Inquiries, etc., displayed by "Operator," "Terminal," or "Date."
Stuck Jobs Report	List of all transactions in EXEC or WAIT 1, 6, 12, or 24 hours after submission. Limitable by TOT, Job Type, Phase, and Status.
Average Daily Transactions	Shows the total of LI, L/LI, LI2, LR, LD, LU, TI, T/LI, TR, TU, TD, T/LI2, TI2, 1X1 Hit, and Sum on a per day basis.
Aborted/Abnormal Transactions	All transactions with an ABORT or REJECT status.
Monthly Hit Report	Tracks monthly hits by transaction type (TOT).
Hit Distribution Report	By date range hits within 1000 point score range. By transaction type (TOT).
Daily Transaction Report	Shows LI, L/LI, LI2, LR, LD, LU, TI, T/LI, TR, TU, TD, T/LI2, TI2, RS, 1X1 Hit, and Sum on weekday average and day of month count total.
Consolidations Report	Details the consolidations recommended completed and erred on MBIS for the selected time frame.
Card Quality Report	Displays the quality and details the number of incoming cards per user and defined date. Separated into criminal and applicant cards.
Operator Usage Report	Shows the terminal ID, date, time of logon, time of logoff, and a total of logged on hours for the selected time frame.
Transaction History Audit	Track transaction history and changes by TCN, Gallery, Event ID/#, or Booking ID/#.
User Activity Report	Generates a report of audited activities generated by user actions.
Folder / Document Activity Report	Generates a report of user activity on a specific archived Folder or Document.
Document Activity Count Report	Report will display count of the following broken by TOT: <ul style="list-style-type: none"> • Count of documents Added • Count of documents Sealed • Count of documents Unsealed • Count of documents Deleted • Count of documents Undeleted
Archive NIST Statistical Report	Displays the count of persons, count of events, count of deleted and sealed persons, count of deleted and sealed events, count of fingerprints, count of palmprints, and a total count.
Audit Trail	Detailed account of all activities by a user in a specified timeframe.

REPORT	DESCRIPTION
User List Report	Report displays all user profile information.
Ad Hoc Query	GUI-based query generation. Provides the ability to access MBIS demographic database and audit. User can create and save a report template that will be available to other ad hoc reporting users.
ADDITIONAL REPORTS	
Call Reports	<ul style="list-style-type: none"> • Summary of all Calls: Opened or Closed, by week or month. • Summary of Calls sorted by problem type. • Individual ticket and ticket contents, including but not limited to: <ul style="list-style-type: none"> ▪ Date and time notified ▪ Name of Service Technician or Engineer ▪ Component (hardware or software service) ▪ Description of problem ▪ Action taken to resolve issue; Action taken to prevent recurrence ▪ Root Cause ▪ Time of completion • Performance Report- Downtime by location per month, by year.

AD HOC REPORTS

Contractor will comply with the **Admin Function 22** stating that the report design by administrators will be provided by the ad hoc models delivered through Jasper reports.

LEVELS OF SERVICE

Contractor will ensure that County staff, the Remote Site administrators, FBI auditors and other authorized personnel are able to inspect the repository, the log of transactions and performance/throughput rates, and user-level access history in order to allow the County to generate predefined standard reports as well as ad hoc reports through Contractor's ISM console. Please refer to the Service Level Proposal (SLP, **DEL-33**) submitted with the Business Proposal.

ASSUMPTIONS

Contractor has shared the list of standard reports available in the ISM which will meet the County's stated requirement. Any other reports, which might be required by the County in future, will need to be custom built using ad hoc report option of ISM. The custom reports will be built using Jasper.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-33: Service Level Plan.**

SECTION 3.2 SUPPORT SERVICES

During the System Operation Phase of the Agreement, as part of System Maintenance, Contractor shall support the operation of the System ("Support Services"), as further provided in this Section 3.2 – Support Services below.

SECTION 3.2.1 SCOPE OF SUPPORT

Contractor's Support Services responsibilities shall include responding to and tracking problems reported, resolving Deficiencies and controlling configuration of software and hardware baselines, on-site and remotely as Necessary.

Contractor shall backup (data and system configurations) daily for COOP considerations. Copies of the backup tapes shall be stored off site from the Primary Site and Disaster Recovery Site to increase the likelihood of their availability in case of a natural or man-made Disaster.

Contractor shall be responsible for all upgrades to the installed operating system(s), database management systems, and application software to ensure that the services conform to future approved FBI EBTS interface specifications and that no service is running on a suite of software no longer supported by the licensing Contractor.

The Contractor shall manage its services to include reports on the status of the System, the services provided, and repository and transaction volumes.

Contractor will comply with the support services requirements of Section 3.2 and Section 3.5 of the SOW.

This section describes Contractor's approach to satisfying the support services requirements, identifies and describes the support services to be provided, staffing, and availability. It also describes Contractor's approach for ensuring that the operational software is kept current with respect to its latest software releases and applicable biometric standards. All requirements are detailed in the attached Service Level Proposal (SLP, DEL-33).

APPROACH

Contractor's service and support mission is to consistently exceed customers' expectations in the implementation, maintenance, and support of products and services within the customer requirements. Our maintenance and support services are designed to be flexible, and able to meet even the most stringent of requirements. Contractor has a team of support personnel in the central Los Angeles area maintaining Contractor's biometric, network and telephony products. Contractor maintains additional support centers in throughout the United States, with our Headquarters in Irving, TX, and our Biometrics Headquarters in Rancho Cordova, CA.

Our Long Beach Office is centrally located in the County of Los Angeles. There are appropriately 60 Contractor personnel reporting to this facility. This includes Sales and Operations Teams, Voice & Data. There are twelve (12) technicians and six (6) engineers dedicated to supporting various Contractor products throughout the County. One major contract they have right now is maintaining the voice and data plan for 13 LA County locations, all of which are law enforcement affiliated. Contractor also maintains a 24 hour parts depot which is approximately 10 minutes from the Long Beach Office. This invaluable technical experience and familiarity with the County substantially enhances

Contractor ability to provide a comprehensive maintenance plan designed to meet the distinct needs of the County and its Remote Sites.

Contractor's Los Angeles County support team, working out of our Long Beach Office, will be utilized in our effort to provide a quick response to all remote sites. This local support team provides us with a unique advantage over others who do not have this type of support presence in the County. Personnel from the Long Beach Office will assist with Level 2 support providing remote workstation and peripheral support throughout the County. Should third-level support be needed, the Level 2 support team will immediately escalate to the engineering group, in Rancho Cordova, CA. All Contractor support functions will operate in a 24x7, 365 days per year environment.

Contractor's support team will also include two dedicated on-site engineers who will be the County's point of contact for all service related concerns.

The support of the County MBIS project is not driven by a cost cutting model but years of experience in support of a geographic distribution and complex management and maintenance requirements. We have proven that we can operate under such circumstances and require no new learning curve to meet the RFP's requirements.

COVERAGE TYPE AND SUPPORT

Contractor's standard MBIS support offering is a four-tiered model, unless otherwise requested, that follows industry best-practices for delivering technical support. The following is a brief description of the four tiers of support:

- **Level 1 Support** – Provided by Call Center personnel assigned as first call responders, initiating Trouble Tickets and related incident information, and ensuring the appropriate Field Support personnel are engaged.
- **Level 2 Support** – Field Support Engineers dedicated to a specific Customer or group of Customers, have specialized knowledge, skills and abilities to resolve most incidents.
- **Level 3 Support** – Systems Engineering personnel dedicated to provide escalation support, engaged (along with management) when normal support processes fail to resolve an incident within the required timeframe.
- **Level 4 Support** – Software Developers primarily dedicated to new product development, however, engaged in support if for some reason Levels 1 through 3 cannot resolve an incident.

Contractor's latest MBIS, with its flexible design, can be easily integrated with Contractor's support processes to ensure that the highest availability can be realized. Automated software notifications to our 24x7 Network Operations Center (NOC) alert Contractor of problems onsite. Contractor's latest MBIS platform allows for an unparalleled "*proactive*" approach to Service and Support, creating a new standard for support in the biometric identification industry. Contractor will provide support services to ensure that the County receives the highest quality of support, including a 24x7 help desk for problem tracking and resolution.

Throughout the life of this contract term, Contractor will provide the County with 24x7 extended coverage support. This service will provide a qualified team of full-time County dedicated engineers providing both support and maintenance services (both corrective

and preventive), who are able to respond onsite within 4 hours of being notified of the outage. They will provide remote access assistance as well as phone and email support. These engineers will be supplemented with trained field engineers from our support office in Long Beach and throughout the Western US for remote and preventive site maintenance. The County maintenance plan will also include advanced remote diagnostics with first and second level support maintenance from the core maintenance team, located in Long Beach, California with escalated back-up support from the Contractor Level 3 Support Team located in Rancho Cordova, California. This support team is staffed with Sr. System Engineers, trained in all aspects of System software and configuration application support. Development Engineers, who provide Level 4 support, are also co-located in the Rancho Cordova, CA facility.

Coverage will be handled in the manner described in Table 23.

Table 23: Site, Coverage, and Conditions

SITE	COVERAGE	CONDITIONS
County Primary Site and COOP Site	24 x 7	<ul style="list-style-type: none"> • 24 x 7 coverage onsite / remote access available, as needed • 1 hour notification to the County for Central Site interruptions for time of call • Notification within 1 hour to the County for Central or Remote service disruptions caused by hardware or software that Contractor has identified. • 4 hour onsite if needed.
Remote Sites	24 x 7	<ul style="list-style-type: none"> • 24 x 7 coverage / remote access / phone support • Acknowledge problem within 1 hour of reported service disruption (Phone or Email) • Notification to the County within 8 hours for Central or Remote service disruptions caused by hardware or software that Contractor has identified. • 4 hour onsite if needed.

CALL CENTER AND DEFICIENCY TRACKING

All problem calls reported by the LACRIS Help Desk or the end user will be reported to a 24 x 7 Contractor help desk through a 1-800 number at the Network Operational Center and dispatched immediately to the dedicated County support team. All calls will be tracked, and users will be provided with a problem ticket number. The County support engineer processes the tickets resulting in closure, update, or escalation of the ticket through the help desk.

The automated system includes the ability to leave detailed voice or email notifications of an outage that will be responded to within 24-48 hours. In addition, as part of maintenance services, the complete County MBIS will be monitored for both hardware and software efficiencies. This monitoring will provide for true 24 x 7 System support and immediate, automatic system call initiation. Contractor will adhere to all response time requirements as they are stated in **Section 3.5.2** and will follow the deficiency priority and correction requirements as stated in **Section 3.5**.

The flow of the support calls are provided in Table 24.

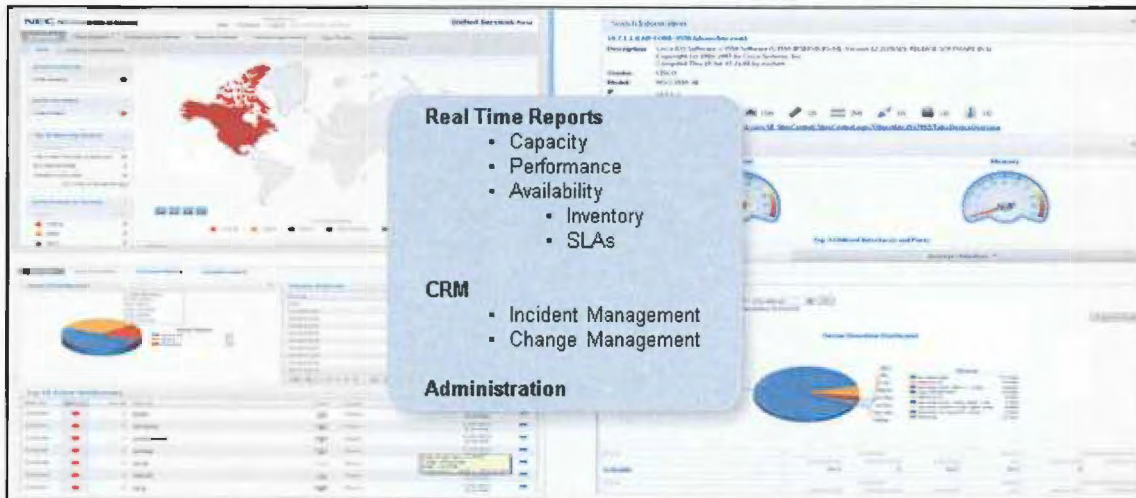
Table 24: Flow of Support

CALL CENTER FUNCTIONS
<ul style="list-style-type: none">• Contractor (RMS) remote monitoring will indicate failure of a device or service. When a monitoring alert occurs, the monitoring service identifies this as a failure item or service alert; and the call is logged into the Contractor Help Desk Problem Call Center. The call is dispatched and worked according to priority by the County-Contractor Support team.• Contractor staff, in the course of their normal daily duties, will identify and respond to an issue with the main system or remote system. A call is then placed and logged into the Help Desk Problem Call Center.• The LACRIS Help Desk or users will call the toll free service number and place their service call, noting the name, agency, and description of the problem to the Contractor Helpdesk. The Call will then be dispatched to the assigned Contractor Engineer. Once the call has been dispatched, the Contractor assigned Engineer will return the call and work the problem issue. Each call placed will received a problem ticket number, and is tracked through the Contractor Helpdesk Problem Call Center.• A call log report, listing all open, closed or escalated calls can be retrieved at any time from the Contractor Helpdesk-Call Center. County will be provided with a customer portal to view status of calls.• Contractor will provide notification to the County office within one hour of receiving the call and providing the service.• TFS Problem Escalation Tracking - All escalated calls are assigned a priority level and will be updated or closed and escalated through the Contractor escalation hotline. Escalation notification will go directly to Engineering's Level 3 and Level 4 Support. Contractor will continue to notify the County staff of any subsequent issues at regular time intervals. For problem tracking and report generation, the County will have access to the Contractor TFS Problem Tracking System through the Web Portal. A problem report log consisting of report number, submitting agency, description, time of call, priority, actions taken, cause and resolution of problem. In addition, the report log will show when all units were installed for both Primary and Remote sites.

WEB PORTAL ACCESS

Contractor provides an online portal for clients to review incidents and tickets, incident and ticket metrics and various reports for monitored or managed components. Additional reports may be included depending upon the contracted services. All reports are viewable on an on-demand basis and many reports are schedulable by LASD. The portal provides a means for LASD to input trouble tickets and change requests, along with the ability to review real-time and near-real-time information regarding their network.

Figure 3: Support Services Web Portal



DEFICIENCY PRIORITY LEVEL

The priority level for each reported deficiency will be assigned based on the Deficiency Priority Level table provided in the SLP (DEL-33) and Section 3 – System Operation of the SOW.

DEFICIENCY ESCALATION

Contractor will also provide a problem escalation system. This system allows tracking of all escalated support issues through the TFS (Team Foundation System). The County will have a web-portal access into this System as described above. The system allows calls to be treated on a priority basis with two types of internal escalation paths, Management and Technical for immediate and proper level of attention. Details of this escalation path are provided in Figure 7.

DEFICIENCY RESOLUTION

Based on the priority assigned to each deficiency, Contractor will respond back to the County within the prescribed timeframe provided in the SLP (DEL-33) and will resolve the deficiency within the specified timeframe also provided in the SLP (DEL-33).

Contractor understands that deficiencies that require an immediate response (Priority Level 1) are System or component failures that prevent subjects from being enrolled, images from being searched or responses from being delivered.

For all Priority Level 1 deficiencies, Contractor will attempt to correct the problem by phone or remote access. If unsuccessful, Contractor will dispatch a technician within four (4) hours of the time Contractor was initially notified. All situations that prevent the initiation (due to access availability) of on-site repair within four (4) hours will be documented in Contractor's electronic report log and reported to the County's Help Desk. Contractor will ensure that the equipment will be repaired within eight (8) consecutive hours.

All Priority Level 2 Deficiencies will be corrected within two (2) Business Days from the time the problem was reported.

See attached Service Level Proposal (SLP, **DEL-33**) for additional deficiency resolution details.

CONFIGURATION CONTROL

Contractor understands the complexities involved with administering and maintaining geographically dispersed systems. Contractor has the experience of handling successfully, many MBIS implementations, which feature remote workstations, that are not only geographically remote, but often, have limited bandwidth connections to the Primary site. To address these challenges we have designed our architecture to centralize the software deployment and rollout. See Section 3.6 for details on Configuration Management.

DATA BACKUP (COOP)

Contractor will backup (data and system configurations) daily for COOP considerations. Copies of the backup tapes will be stored off site from the Primary Site and COOP Site to increase the likelihood of their availability in case of a natural or man-made disaster.

CONFIGURATION AND FACILITATING UPGRADES

Contractor shall use Team Foundation Server (TFS), a web-based bug tracking system which integrates tightly into the development, support, and QA internal processes to automatically generate system e-mails upon a status change for issues logged within the system or upon a status change for a defect or issue. For example, if a software defect is discovered and logged, the initiating party will receive email notification when work has begun on the issue, when the item is released for QA, and when the item is released to be installed at the production site. Configuration and Patch Management to resolve trouble ticket issues or reported defects will use the same tools as defined in Section 3.6 (Configuration Management) of this document. The tool for managing and maintaining the configuration and revision control for each site is Microsoft's System Center Configuration Manager (SCCM). Using SCCM, the County support team can tightly control the release, installation, and maintenance of the software components in use.

Contractor will provide available updates to installed Operating Systems, database managements systems, and applications software to ensure that the services conform to the future approved FBI and County EBTS interface specifications. Contractor will apply all security patches and updates and no service will run on software no longer supported. Contractor's product development and maintenance policy is driven by two equally important paths: 1) Biometrics industry requirements including adherence to standards such as the EBTS 9.3 standard required by the County; and 2) IT-related advancements, including advancement to operating system, relational databases and middleware while paying attention to third party life cycle management. These two paths combine to generate a release of the Contractor's MBIS product which is quality controlled and released to the County and other Contractor customers. Therefore, there may be instances where availability of an IT-related advancement may not make its way immediately to the Contractor product release due to requirements of integration, validation and certification of such IT-related issues on our generic product.

SYSTEM REPORTING

System reports include system performance status, problem reporting, statistical reports, transaction volumes, and repository growth rates for system storage.

LEVELS OF SERVICE

Please refer to the Service Level Proposal (SLP, DEL-33).

ASSUMPTIONS

- The LACRIS Helpdesk personnel have the expertise to work with the Web Portal and handle routine maintenance calls.
- The LACRIS Helpdesk personnel understand the deficiency resolution policies.
- The County will provide an offsite storage area or facility where the backup media can be stored.

RISKS

Table 25: Support Services Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Contractor understands that to initiate a maintenance call, the County will place calls through the call center. A possible risk is a break down in this communication.	The County personnel will have the lead Customer Support Engineer's and Support Manager's contact information. This process will ensure that the incident is addressed and Contractor support notified.

APPLICABLE STANDARDS

Contractor is a process driven, policy oriented vendor. Our comprehensive policies govern such activities as:

- Access to customer networks only by security cleared personnel
- Information Security, ensuring the safeguarding of customer data and the use of anti-virus software
- Physical Security of our data centers and networks

For System Support, the most visible policy is adherence to CJIS Security Policy version 5.2. All Contractor staff undergo fingerprint based background checks at the State and Federal levels. Prior to beginning work on a project, staff are also required to attend the requisite CJIS training provided by our on-staff CJIS Systems Officer (CSO).

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- Service performance at or above the agreed levels. We will support the System on a 7 x 24 schedule and meet the System uptime requirements.
- **DEL-33: Service Level Plan.**

SECTION 3.2.2 CUSTOMER SUPPORT

As part of its Support Services, Contractor shall provide operational support for the Solution 24 hours per day, 7 days per week (24/7) ("Support Hours"), which shall include without limitation providing a point of contact for all System problems by maintaining a System for customer support ("Customer Support"). Such operational support shall include Support Services to correct any failure of the Solution and to remedy Deficiencies in accordance with Section 3.5 – Correction of Deficiencies of the SOW to ensure that the Solution operates in accordance with the Specifications, including System Requirements, warranties and other requirements under the Agreement. Requests for Customer Support will be submitted by County's technical support via telephone and/or Contractor's web-based trouble ticketing system. In the event that the Contractor's web-based trouble ticketing system is not available, County may use email or any other reasonable means to request Customer Support.

In addition to the requirements specified in the System Requirements Specifications, Contractor's Customer Support Service Level Requirements shall also include, but not be limited to, those listed below, as follows:

- County designated staff shall have access to Contractor's Customer Support through the web-based trouble ticketing system or telephone. The trouble ticketing system shall provide for County a simple method to submit, track and update issues that require escalation to Contractor's Customer Support. The authorized County contacts will each receive an account and training on the ticketing system.
- Contractor shall provide a telephone number for County staff to call during Support Hours. This telephone number shall be managed by an automated system to quickly contact Contractor's County staff with the appropriate Customer Support personnel.
- Contractor's automated system shall include the functionality of leaving detailed voice mails describing the issues. The voice mails must be responded to within 24 to 48 hours (excluding weekends and holidays).
- Priority Levels for the Deficiencies shall be assigned according to definitions specified in Section 3.5.2 – Deficiency Priority Levels.
- Contractor shall respond within the period specified in Section 3.5.2 – Deficiency Priority Levels depending on the Priority Level of the Deficiency.
- Contractor's Customer Support shall made be available to County during Support Hours on a 24/7 basis.
- Contractor's Customer Support shall work with County's Project Manager and County's technical support staff on correcting Deficiencies and keep such County personnel informed regarding the updates and scheduled timeframes to ensure that all maintenance windows are clearly communicated and the requirements of this SOW are met.
- Deficiency correction, timeframes and Service Credits for failure to timely correct any Deficiencies as specified herein shall be as specified in Section 3.5 – Correction of Deficiencies.

SECTION 3.2.3 SERVICE LEVEL PERFORMANCE

Contractor shall ensure that, during the term of the Agreement, the MBIS shall provide at least 99.8 percent (99.8%) availability for all Services ("Service Availability"), measured monthly, and in accordance with the terms of the Agreement, including all Service Level Requirements set forth herein.

Contractor will comply with the Service Level Requirements of Section 3.2.3 – Service Level Performance of the SOW.

This section and the attached Service Level Proposal (SLP, **DEL-33**) describe Contractor's approach to satisfying the service level requirements. In the Service Level Proposal, we identify the proposed services and the proposed levels of service associated with each.

APPROACH

Contractor's extensive experience with major AFIS and MBIS statewide and international installations demonstrates a successful track record of our ability to meet or exceed the County Service Level Requirements. Contractor fully complies with the requirements for service level performance set forth in Section 3.2.3 – Service Level Performance of the SOW and the SLP (**DEL-33**).

Contractor will ensure during the life of the contract, including any optional year extensions, that LASD will be provided with 24 x 7 support with an availability of greater than 99.8% during any calendar month.

With Contractor's latest technology, the above referenced SLAs will be accomplished using the highly available clustered servers, RAID 6 SANs implemented on a virtualized cloud platform. The County central site uses multiple Contractor Integrated Enterprise System Bus (iESB) technology services. Contractor Provisioning Center, and vCenter™ running on multiple VMware ESXi and executing on clustered high availability redundant servers are all examples of all the technologies we bring to bear to meet the SLAs. Using this environment, both the central and remote sites will be able to address most preventive maintenance requirements without actual downtime to the customer.

LEVELS OF SERVICE

Please refer to the Service Level Proposal (SLP, **DEL-33**).

ASSUMPTIONS

Contractor assumes:

- The number of records and average size of each record stated in
-
- Table 1 and
- Table 2 based on the information provided in the RFP are correct. In the event the peak hour transaction count in
- Table 5 is exceeded for a period of time, the response time commitment may be relaxed proportionately for that limited period of time as mutually agreed to by the parties.

- Repository and probe images meet the requirements in Table 7 for the accuracy testing.
- The system expansion design is based on a 2% growth rate for all components of the System as specified by LASD in the RFP requirements and answers to questions.
- Contractor assumes EBTS records are received in an industry standard NIST/California EBTS format. This includes tenprints, latents, palmprints, mugshots and associated demographic data.
- Non-NIST records (documents, photographs, etc.) will be in an industry standard format.

RISKS

Table 26: Service Level Performance Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Database Quality affecting system accuracy	Contractor will encode multiple events and maintain a best image composite for each individual in the MBIS database. Additionally we will employ multiple matching algorithms and multi-stage matching processes, including template and score fusion.
Transaction Image Quality affecting system accuracy	Contractor will perform full quality assessment on incoming records and will use image enhancement algorithms, multiple matching algorithms as well as template and score fusion.
Variance in latent examiner encoding	Contractor will provide extensive best practice training to enhance latent examiners' expertise.

APPLICABLE STANDARDS

- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- Electronic Biometric Transmission Specification (EBTS), NGI-DOC-01078-10.0.
- IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- NIST Best Practice Recommendation for the Capture of Mugshots. Version 2.0. September 23, 1997.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.
- California Department of Justice (Cal-DOJ) Live Scan Transmission Standards

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-33: Service Level Plan.**

SECTION 3.2.4 TRAINING

Contractor, in conjunction with third parties and cooperation from County, will develop those Training Plan(s) and materials and will conduct those training activities identified as Contractor responsibilities [DEL-17] of the System Implementation Phase of this SOW.

Contractor will comply with the training requirements of Section 3.2.4 – Training of the SOW.

This section describes Contractor's approach to satisfying the training requirements, including proposed activities, training schedule, deliverables, descriptions of deliverable content, and methods and tools to be used. It also identifies the risks inherent in the training approach and its mitigation strategies.

APPROACH

Contractor will work with LASD to develop the training plan and materials tailored to LASD's needs. The following sections demonstrate the methodologies and tools used in the MBIS training program. CONTRACTOR fully complies with the requirements for training set forth in Section 3.2.4 – Training of the SOW.

Our training approach is based on nearly 30 years of experience in law enforcement market and training of multiple users. Our training approach will consist of the following activities:

Table 27: Training Approach

TRAINING APPROACH	
<ul style="list-style-type: none">• General overview of MBIS• Provide User Guides to each participant• Technical Discussions• Quick Start/Quick References• Best Practices• Hands-on demonstration of screens, menus, and toolbars• In-depth, hands-on operation by trainees	<ul style="list-style-type: none">• Mock Scenarios• Question and Answer Session• Test – Written and hands-on operation• Final Review• Training Evaluations• Training Certificates• Additional reinforcement training

Consistently applied, Contractor has found that these approaches provide the best result leading into a successful operation with multiple identifications. Contractor will coordinate with LASD on release of MBIS reference training materials.

EVALUATIONS AND CERTIFICATIONS

Contractor's certification process is tailored to LASD's requirements for course and student evaluations. Contractor offers a two-fold approach to our certification process: (1) attendance, and (2) competency. Attendance-based evaluation certificates, confirming that the attendee completed the required class hours, will be issued at LASD's request. Performance-based ratings are not included in this attendance document. Most agencies use these certificates for meeting mandatory "continued training" requirements.

Performance-based certificates, however, are issued following performance review by the Training Manager, and certify the attendee successfully completed the class requirements. Scenario testing and as required written tests for these certificates measure expected skill outcomes.

TRAINING MATERIALS

The following training materials will be provided to accompany the courses described in the Contractor Training Curriculum. Additional training aids include quick reference guides, checklists, and training evaluations for each course. Contractor will provide a fully-integrated online help system containing user documentation for each MBIS workstation type or application. All documentation will be preloaded on all MBIS workstations and easily accessible to users.

Table 28: Training Course and Support Materials

DESCRIPTION	MATERIALS
Tenprint Course	<ul style="list-style-type: none"> • Automated Tenprint User Guide • Automated Tenprint Quick Reference Guide • Manual Tenprint User Guide • Manual Tenprint Quick Reference Guide
Latent Course	<ul style="list-style-type: none"> • Latent User Guide • Latent Quick Reference Guide
Archive Course	<ul style="list-style-type: none"> • Archive User Guide • Archive Quick Reference Guide
LACRIS Help Desk Course	<ul style="list-style-type: none"> • LACRIS User Guide • LACRIS Quick Reference Guide
System Administration Course	<ul style="list-style-type: none"> • System Administration User Guide • System Administration Quick Reference Guide
Support Materials and Job Aids	<p>The following support materials and job aids will be provided:</p> <ul style="list-style-type: none"> • Tenprint Automated Checklist • Tenprint Manual Checklist • Latent Checklist • Archive Checklist • System Administration Checklist • Training Evaluations • Written Tests • Hands-on exercises • On-line Help
LASD-Supplied Training Tools	<p>In order to support the training, the following items will need to be provided by LASD.</p> <ul style="list-style-type: none"> • New tenprint records – fingerprints and palmprints • Latent lifts – fingerprints and palmprints • LASD-registered tenprint records

RISKS

Table 29: Training Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Operator Turnover	Re-occurring training is scheduled to be accomplished yearly.
Training Facility Readiness	Prior to training, the training manager will collaborate with the LASD and Contractor project managers to ensure that the training facilities are fully equipped and ready for the different training courses.
Training Latency	The period of time between the training and productive use of the training may be of a duration causing lack of retention; Contractor supplies initial training as concurrent to deployment as possible.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-17:** Training Plan
- **DEL-19:** Training materials
- **DEL-11:** User Manuals

Please refer to Table 28 for a list of materials provided per training course.

SECTION 3.3 PROGRAM MANAGEMENT

The sections under this Section 3.3 – Program Management below describe the required program management functions to be performed by Contractor throughout the System Operation Phase of the Agreement.

Contractor shall document management organization, roles and responsibilities, resources, processes, and other pertinent management information in a Project Management Plan [DEL-01] and maintain that plan current throughout the System Operation Phase of the Agreement.

SECTION 3.3.1 PROGRAM ORGANIZATION

Contractor shall establish a formal Contractor Program Management Office (“PMO”) responsible for executing the total effort required under the Agreement. A clear line of program authority shall exist among all organizational elements, including subcontractors. Roles, responsibilities, authority structures and reporting requirements shall be established for each organizational element.

Contractor shall appoint a Contractor’s Project Manager or Program Project Manager (“PPM”) who shall be responsible for accomplishing all tasks to be performed under the Agreement. The PPM shall be responsible for Contractor’s technical, cost and schedule performance. The PPM shall have full authority over all Contractor program activities and resources. The PPM shall be the principal interface between the program and Contractor’s corporate organization, between the program and its associated contractors, and between Contractor and County for all matters

relating to the Agreement. The PPM, or designee, shall be available to County management on a 24/7 basis.

Contractor will comply with the program organization requirements of Section 3.3.1 – Program Organization of the SOW.

This section describes Contractor's approach to satisfying the program organization requirements, describes the proposed PMO, how the proposed PMO (including subcontractors and vendors) is organized (including an organizational chart); how it fits into Contractor's overall corporate structure (an organizational chart is included); indicates how the proposed PMO will interface with the County; and discusses the responsibilities of key personnel. This section also identifies and discusses the principal interfaces and reporting mechanisms internal to and external to the PMO as well as elements of the Proposer's support organization.

APPROACH

As a solution company, Contractor is offering a structured and proven management team, with comprehensive support and maintenance methodologies. These Support and Maintenance strategies offer a meaningful and systematic approach to providing a reliable performance level, deemed necessary, in mission critical systems such as the County's MBIS. In order to provide this all inclusive type of operational support, Contractor is providing the necessary structure, oversight, and management which is critical for the smooth transition from implementation to quality operational support through the contract life cycle, and will document that in the Project Management Plan (PMP – DEL-01) and update that plan as needed.

Contractor fully complies with the requirements for Program Organization set forth in Section 3.3.1 – Program Organization of the SOW, which describes the proposed Program Management Organization (PMO) and how it satisfies the County's requirements.

Table 30: Comprehensive System Operation Program Documentation

SYSTEM OPERATION PROGRAM DOCUMENTATION	
<ul style="list-style-type: none"> • Product Life Cycles • Preventive Maintenance Procedures Including Daily, Weekly, Monthly, Quarterly and Annually • Equipment Inventory • Service Support Procedures per Sub system <ul style="list-style-type: none"> ▪ Backup and recovery ▪ Configuration ▪ Support procedures 	<ul style="list-style-type: none"> • Spare Parts Provisioning • Remedial Maintenance Procedures • Installation Process and Procedures • System Configuration Documents (Primary Site, COOP Site, Remote Sites. • Problem Reporting • System Network Design • Patch Deployment Process

This includes all devices for the System Operation and Support of the Primary Site, Remote Sites, COOP Site, and remotes, as well as monitoring of the performance and status of all elements of the system. Contractor will detail the standards, process, and experience required to support the County customers both during the upgrade and on an ongoing basis though the life of the new system.

PROJECT STAFFING

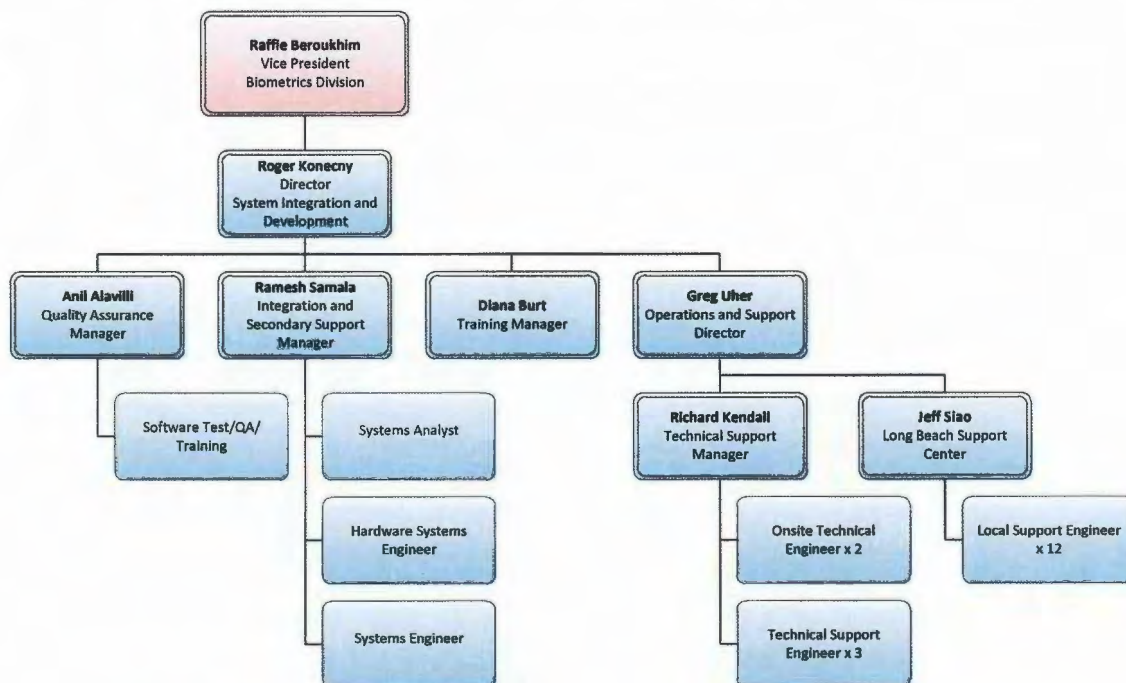
This section describes Contractor staffing for the support team. It includes the key personnel and corporate organization.

MBIS System Operation Team

Contractor will staff the MBIS System Operation team with an experienced maintenance and support staff that has knowledge of the current locations, data, and users. These key members will be dedicated to the successful operations of the County MBIS in an ongoing basis.

The MBIS System Operation Team depicted in Figure 4 will be composed of engineering, service and integration personnel that will support the operations of the primary, alternate, and Remote Sites with the participation of both QA Manager and overall Service Delivery Manager. This team will provide experienced integration personnel not only on Contractor products but experienced with biometrics, interfaces, and operations. This will ensure the operations and reliability required for a best in class public safety organization.

Figure 4: MBIS System Operation Team



Key Personnel

Table 31 provides the key system operation support personnel assigned to the project and provides a brief summary of their responsibilities. These team members are responsible for ensuring that the County MBIS support functions are maintained at optimum levels.

Table 31: Roles and Responsibilities of Key System Operation Support Personnel

ROLE	RESPONSIBILITY	NAME
Project Executive Sponsor	<ul style="list-style-type: none"> • Provides interface to CEO and senior management • Understands client business needs • Manages and negotiates contract terms and conditions. 	Raffie Beroukhim
Project Director	<ul style="list-style-type: none"> • Totally responsible for compliant execution of the contract, possessing due authority and responsibility over all resources required for such execution • Provides overall leadership of the project team and single point of contact for the County Project Director and executive staff • Works with the County Project Director and agency representatives to ensure timely and effective responses to information requirements and to resolve actual and/or potential problems • Primary technical liaison with the County project team with responsibility for defining and obtaining concurrence for implementation of total project. 	Roger Konecny
Integration Manager	<ul style="list-style-type: none"> • Develops the Conversion Plan, with ongoing coordination to maintain and update the detailed plans and procedures as necessary to accomplish the successful conversion and loading of system data • Primary conversion liaison with the County project team with responsibility for developing detailed procedures for record handling and tracking during conversion and providing regular status reporting on conversion activities • Direct management and technical oversight of the conversion, database loading, conversion verification/validation, and delivery of the converted data • Primary responsibility for planning, coordinating, and accomplishing system delivery preparations, system delivery, and installation • Direct involvement in the preparation of formal test plans for pre-delivery, installation, and formal acceptance testing, and leadership of all formal testing activities • Quality assurance of system deliverables and associated technical documentation. 	Ramesh Samala

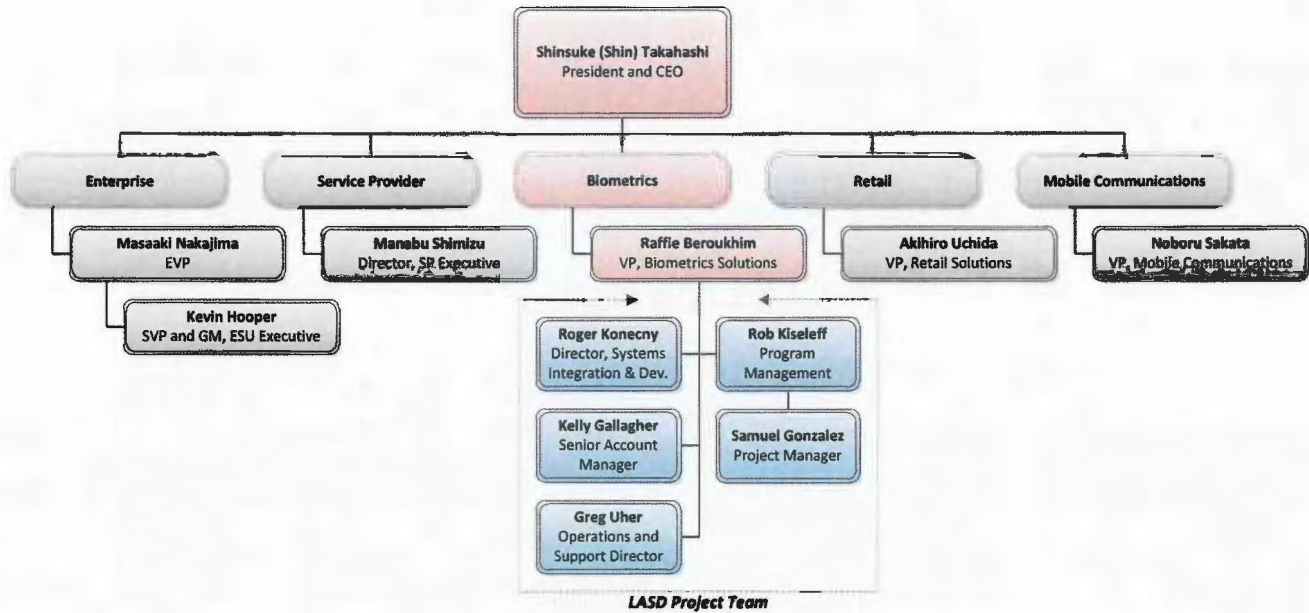
ROLE	RESPONSIBILITY	NAME
Training Manager	<ul style="list-style-type: none"> • Develops the Training Plan, with ongoing coordination to maintain and update the detailed plans and procedures as necessary to accomplish the delivery of all required training • Primary training liaison with the County project team, with responsibility for developing detailed delivery plans and content requirements for each training course, and for providing regular status updates • Coordinates training schedules and prepares activities • Oversees and directs training delivery and leaders training assessment activities. 	Diana Burt
Operations and Support Director	<ul style="list-style-type: none"> • Primary responsibility for the Operations of the project • Provides the leadership to the Operations Team • Reports to the Project Manager and will support coordination of Operations responsibilities • Primary Operations liaison with the County project team with responsibility for defining and obtaining concurrence for implementation of the Operations. 	Greg Uher
Long Beach Support Center	<ul style="list-style-type: none"> • Manages a Team of 12 Support Engineers • Provides second level support for remote workstations • Provides installation support for remote workstations and central site • Provides Preventive Maintenance and Remedial support. 	Jeff Siao
Service Delivery and Maintenance Support Manager	<ul style="list-style-type: none"> • Supports the Operations and Support Director and assist in planning, coordinating, and accomplishing system delivery preparations, system delivery, and installation • Develops the Operations and Maintenance Support Plan, with ongoing coordination to maintain and update the detailed plans and procedures as necessary to accomplish the effective delivery of operations and maintenance support • Secondary technical liaison with the County project team, with responsibility for planning, coordinating, and implementing the operations and maintenance support capabilities • Participates in training preparation and delivery for providing operations and maintenance 	Larry Moran

ROLE	RESPONSIBILITY	NAME
	support training for system administrators and support staff <ul style="list-style-type: none"> Oversees and directs the operations and maintenance support activities during the production period. 	
Operations and Technical Support	<ul style="list-style-type: none"> Second level support with responsibility for planning support, coordinating, and implementing the operations and maintenance support capabilities Participation in training preparation and delivery for operations and maintenance support Oversight and direction of the operations and maintenance support activities during the production period. 	Onsite x2
Quality Assurance Manager	<ul style="list-style-type: none"> Reports to Program Manager and ensures both the project deliverables and product meet or exceed requirements for quality Assists in development of final plans for testing and integration Reviews all project deliverables for compliance with contract. 	Anil Alavilli

Project Corporate Organization

Figure 5 depicts Contractor staff who will contribute to the project. Each group or person will play a role according to their specialty and contribution. The solid line between roles indicates the project reporting structure.

Figure 5: Project Corporate Organization



RISKS

Table 32: Program Organization Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Change in Key Personnel	In the event that a change is made to the original resources, Contractor will ensure that the County is notified and the new personnel go through a formal onboarding process, as described in the Communication Management Plan.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-01:** Project Management Plan.

SECTION 3.3.2 MANAGEMENT AND TECHNICAL REPORTING AND REVIEWS

Contractor shall conduct management and technical reviews and provide management and technical reports throughout the System Operation Phase of the Agreement. Contractor is cautioned that the content of reviews shall be limited to that which is sufficient to establish the adequacy of the products and services required under the Agreement. Sales presentations, new product demonstrations and other promotions are discouraged unless expressly requested by County. Contractor shall log all transaction and System activity Necessary to evaluate Agreement performance, facilitate trend analysis and support System and other transactional analysis [DEL-31]. Contractor shall supply appropriate quality assurance and audits to ensure that logs are complete and accurate.

Contractor shall participate in a program kickoff meeting at a County facility 30 days prior to the scheduled date for declaring County's Initial Operational Capability ("IOC"). The purpose of the meeting is to introduce key County and Contractor operations and operations support personnel, discuss plans, examine the status of any risks or issues and address any other issues that County and/or Contractor may wish to discuss.

County and Contractor shall meet at least weekly in person, by telephone or through the provision of e-mail updates exchanged between their respective Program Managers unless the parties otherwise mutually agree in writing via their respective Program Managers. Attendees at the meetings will include County and its staff and Contractor and subcontractors personnel, as determined by County and Contractor management. The objectives of the weekly meetings are (i) to confirm that the program is not encountering technical problems that would cause the program to fail to maintain the agreed-upon service levels, (ii) to provide immediate feedback to the parties to permit any issues to be resolved on a timely basis, (iii) to provide a contemporaneous record showing that the parties have acted to ensure that the program is progressing in accordance with prior agreements, and (iv) to ensure that parties are proactively identifying and addressing issues that could adversely affect service levels.

Contractor will comply with management and technical reporting and reviews of Section 3.3.2 – Management and Technical Reporting and Reviews of the SOW.

This section describes Contractor's approach to satisfying the reporting and reviews requirements, identifies proposed reviews, their purpose, frequency, participants, and any associated deliverables. It also describes the standard reports, their contents, the frequency of reporting, and the recipients (organizations) of the reports specified.

APPROACH

Contractor will provide management and technical reports, as per of the reviews throughout the operational phase of the contract. This section describes the technical review process and the management review process.

TECHNICAL REVIEWS

The technical reviews will include a weekly status meeting and formal semi-annual Operational Program Management Reviews (OPMRs).

Thirty days prior to the scheduled date of declaring the County's Initial Operational Capability (IOC), Contractor will participate in the Kick-off meeting at the County facility. Table 33 presents the Kick-off meeting tasks.

Table 33: Kick-off Status Meeting Tasks

KICK-OFF STATUS TASKS	
<ul style="list-style-type: none">• Introduce key County and Contractor provider personnel• Discuss any Plans	<ul style="list-style-type: none">• Examine the status of any risk or issues, if known• Address any other County/ Contractor issues which need discussion

Contractor will meet with the County on a weekly basis, either in person, email, or telephone. Meeting attendee's will include Contractor's respective project managers, County and County consultants, pertinent Contractor personnel, as well as any Contractor sub-contractors. Table 34 details tasks items.

Table 34: Weekly Status Meeting Tasks

WEEKLY STATUS TASKS	
<ul style="list-style-type: none"> • Confirm program is not encountering any problems which would cause Contractor not to meet its service levels. • Provide any feedback to the parties to permit any issues to be resolved in a timely manner. 	<ul style="list-style-type: none"> • Provide Contemporaneous record showing that the parties have acted to ensure that the program is progressing in accordance with prior agreements. • Ensure parties proactively identify and address issues that could adversely affect service levels.

Contractor will also conduct semi-annual OPMRs. Attendees for the meeting should include County and County consultants, Contractor, and Contractor subcontractors. The first OPMR will be held within 60 days after the IOC. Table 35 addresses OPMR tasks.

Table 35: OPMR Review Tasks

OPMR REVIEW TASKS	
<ul style="list-style-type: none"> • Performance against SLAs • Financial and schedule status • Planned activities • Action items • Problem report status • Configuration management and QA reporting • Issues and risks • Service level shortfalls and plans for corrective action 	<ul style="list-style-type: none"> • Address selected technical and programmatic topics • Contractor will provide rooms for meetings held at Contractor with County staff and will also provide a room for County-only meetings • Make available key personnel as necessary to carry out an efficient and effective agenda • Contractor will furnish meeting agendas, presentation materials, and minutes (DEL-07, DEL-08, and DEL-09)

At a minimum, Contractor will attend and participate in semi-annual meetings of the County Executive Board and the annual meeting of the County Operations Committee held in various locations within the Remote Sites announced in advance.

MANAGEMENT AND TECHNICAL REPORTS

Contractor will log all transactions and System activity necessary to evaluate and validate contract performance, facilitate trend analysis, support the operational System, and provide available transactional analysis. Contractor will provide the needed quality assurance and audits to ensure the capture logs are accurate and as complete as possible. Table 36 lists the required deliverables and timeline for these meetings.

Table 36: Deliverables and Timeline

REQUIRED DELIVERABLES		DELIVERABLE TIMELINE
DEL-07	Agenda	5 working days prior to meeting
DEL-08	Presentation Material	Draft within 5 days prior to meeting Updates during the meeting With final, as part of DEL-09
DEL-09	Minutes	Draft 2 days after the meeting With updates at the meeting and Final 5 days after receipt of County Comments

ASSUMPTIONS

Successful execution of the communication activities described in this section is dependent upon timely participation and support of key LASD and Contractor resources and stakeholders.

RISKS

Table 37: Reporting and Review Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
During the transition to operations: insufficient knowledge transfer to operations staff impacts support.	<ul style="list-style-type: none"> • Involve key support staff throughout the life of the implementation project • conduct formal knowledge transfer and training for all operations staff • clear reporting of status, risks and issues at the IOC by the implementation project management team

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes
- **DEL-20:** Technical Report
- **DEL-31:** System Performance Report.

SECTION 3.3.3 FACILITY PERSONNEL

Contractor shall be responsible for all Primary Site and COOP Site personnel and exercise all rights, responsibilities and prerogatives associated therewith, as Necessary to provide Work under the Agreement. Contractor's personnel shall be subject to the security provisions outlined in Section 3.3.4 – System Security below.

Contractor will comply with the facilities requirements of Section 3.3.4 – System Security of the SOW.

This section describes Contractor's approach to satisfying the facilities requirements, including deliverables and descriptions of deliverable content.

APPROACH

Contractor understands that the County's MBIS Central Site System will be housed in LASD's Norwalk facility. Contractor will work with LASD to ensure the facilities meet all requirements of the SOW. Contractor also understands that LASD will have a significant number of remotes workstations and sites. Contractor will work with LASD to ensure a seamless installation and integration to the main site.

The COOP Site location needs to be determined. Optionally, the County can choose to house the COOP site in the Contractor Rancho Cordova facility. This secure facility houses the Contractor Biometrics team that includes engineering, development, training, operations, and management staff groups and fully complies with the System security requirements of the SOW. The letter confirming Contractor's CJIS Security compliance is provided in the In-Plant Security Plan (DEL-10).

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-01:** Project Management Plan
- **DEL-22:** COOP Plan
- **DEL-33:** Service Level Plan.
- **DEL-10:** In-Plant Security Plan.

SECTION 3.3.4 SYSTEM SECURITY

Contractor shall take reasonable security precautions approved by County, by providing among others the Necessary Software Updates, to ensure the MBIS, including its related hardware, software, data and third-party components, are maintained in accordance with contemporary best business practices, including performing antivirus updates, software updates, configuration management, backup/restore/recovery, System logging and report generation. Contractor shall take reasonable security precautions as approved by County to ensure County's Primary Site and COOP Site physical security.

Contractor shall comply with all provisions of the FBI CJIS Security Policy as specified in Section 1.3.2 – Specifications, Standards and Guides of the SOW.

Contractor shall take reasonable precautions to prevent the loss of or alteration to County's data. Accordingly, Contractor shall keep backup copies of all of County's data in a safe and secure off-site facility approved by County.

Contractor shall not utilize, or provide to third parties, County's database without prior written approval of County.

Contractor shall be responsible for ensuring that appropriate encryption or other security methods are implemented to guarantee the secure transmission of data in the MBIS, as further provided elsewhere in the Agreement including the System Requirements Specifications.

Contractor shall afford County the opportunity to interview and investigate the personnel proposed by Contractor prior to granting them security access to County systems and sites, and County reserves the right to reject their access to MBIS equipment, files or site locations whenever Contractor personnel fail to maintain a clean criminal record or pass a background update procedure administered by and satisfactory to County, as further provided elsewhere in the Agreement including the System Requirements Specifications.

Contractor shall work with County, CalDOJ, Nlets and Remote Site agencies to achieve end-to-end security for all components that make up the MBIS. Contractor shall document its security program in an In-Plant Security Plan [DEL-10].

Contractor shall also notify County in writing within five (5) calendar days of Contractor's knowledge of the existence of any intrusions or other security problems or breaches that may affect the integrity of the System Data or any other County data, subject to the provisions of Paragraph 18 (Confidentiality and Security) of the Base Agreement.

Contractor will comply with the security requirements of Section 3.3.4 – System Security of the SOW.

This section describes Contractor's approach to satisfying the security requirements, including deliverables, and descriptions of deliverable content.

APPROACH

Contractor's MBIS design meets all CJIS Security Policy v5.3 or later, and has the flexibility to meet all of LASD's security policies. Contractor believes MBIS and the workstations will be in physically secure locations that already meet security requirements. For access from outside the CJIS firewall Contractor provides, in addition the strong passwords meeting FBI Security Police, FIPS 140-2 compliant encryption for data in transmission and data on the mobile device. Mobile devices can also use Contractor application level advanced authentication using fingerprint or face recognition or it can use the LASD enterprise advanced authentication.

The Contractor hosted data recovery data center is already CJIS compliant and has passed the FBI audit. The communications between the DR site and primary site will be on a private WAN already used for CJIS information or it will be encrypted with FIPS 140-2 algorithms to meet the FBI security policy requirements.

For complete details, see the In-Plant-Security Plan (DEL-10), provided with the Business Proposal.

PERSONNEL SECURITY

Contractor personnel, contractors, and agents accessing (physically or electronically) the LASD System, LASD computer rooms, Primary Site or COOP Site, and other County facilities where MBIS equipment is installed, shall be required to abide by the CJIS Security Policy, CJIS Security Addendum, and LASD Security Policy requirements.

SITE SECURITY

The physical security controls of the LASD Primary Site located in Norwalk, California and the alternate COOP Site will adhere to the same guidelines described within this document, while adhering to the CJIS Security Policy, CJIS Security Addendum, and LASD Security Policy. This includes physical site security (primary and COOP sites) and technical security measures.

For access from outside the CJIS firewall, Contractor provides, in addition to the strong passwords meeting FBI Security Police, FIPS 140-2 compliant encryption for data in transmission and data on the mobile device.

CONTRACTOR SUPPLIED AND SUPPORTED EQUIPMENT

All equipment provided and serviced by Contractor, whether purchased or covered under a service agreement, will be provided with all the security provisions outlined within this document and will follow associated guidelines. This includes OS Security Patches, sensitive-information security, antivirus software, and security of LASD property in Contractor control.

ASSUMPTIONS

- LASD will maintain CJIS Security Policy v5.0 or later at the Primary Site.
- If the COOP Site is located within LASD, LASD will maintain CJIS Security Policy v5.0 or later.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-01:** Project Management Plan
- **DEL-22:** COOP Plan
- **DEL-33:** Service Level Plan.

SECTION 3.4 MAINTENANCE SERVICES

During the System Operation Phase of the Agreement, as part of System Maintenance, Contractor shall provide maintenance of the System, including the provision of Software Updates and Hardware Upgrades, as further provided in this Section 3.4 – Maintenance Services below.

Contractor will comply with the maintenance requirements of Section 3.4, Section 3.4.4, Section 3.4.5, Section 3.5, Section 3.5.1, Section 3.5.2, and Section 3.5.3 of the SOW.

This section and the attached Service Level Proposal (SLP, **DEL-33**) describe Contractor's approach to satisfying the maintenance requirements, plans for periodic maintenance (inspection, adjustment, and replacement of defective parts) at the primary site, and the COOP Disaster Recovery site. The description includes the frequency of visits, service availability, and proposed working hours. It also describes plans for remote site maintenance, including response times for on-site maintenance, procedures to be used to log problem reports, to notify County of problems and their status, and to escalate problem reporting.

APPROACH

Maintenance Services is tightly integrated with and is a part of, Support Services. Contractor's service and support mission is to consistently exceed customers' expectations in the implementation, maintenance, and support of products and services within the County defined customer requirements. Our maintenance and support services are designed to be flexible, and able to meet even the most stringent of requirements. Contractor is the only vendor to have provided a successful operational model of this size, complexity, and magnitude. To maintain this consistency, all hardware, software, engineering and development support is now directly handled out of the Rancho Cordova, CA facility. Contractor will fully comply with the maintenance requirements as set forth in Section 3.4 – Maintenance Services of the SOW.

SCOPE OF MAINTENANCE

Contractor will provide the County with a comprehensive maintenance service package designed to keep all County's MBIS equipment, in optimal operational condition. As part of the maintenance service package, Contractor will provide 24 x 7 support for the County Primary Site, COOP Site, and Remote Sites.

All Service Support calls will be routed through a centralized problem call / dispatch center and dispatched to the appropriate Contractor-County support team member. Direct email or phone support may be sent to the Contractor-County support team; however, for statistical reporting purposes, all service calls must be logged into the call collection system.

PERIODIC PERFORMANCE MONITORING

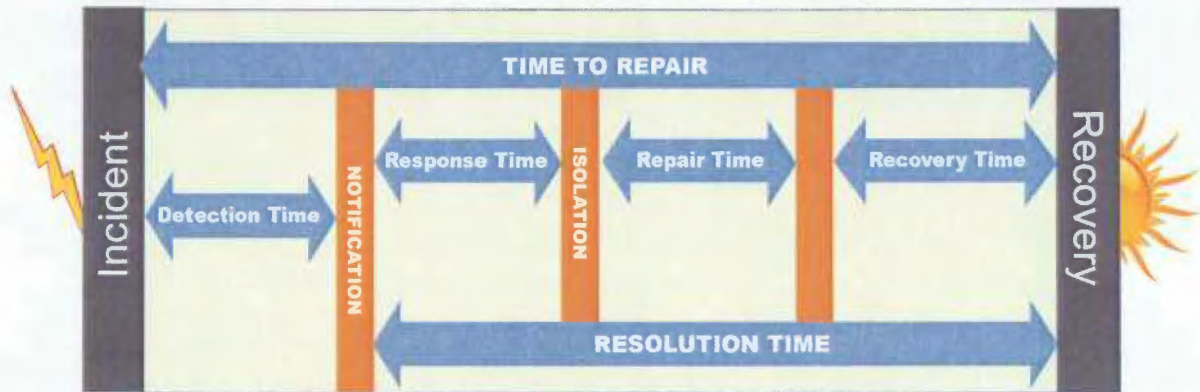
Contractor will be responsible for periodic monitoring of System performance. All server systems, County Primary Site, COOP Site, and Remote Sites will be monitored using a "real-time" remote management service (RMS). Working in conjunction with our preventive and remedial maintenance programs, the RMS service will be an added feature providing advance alerts to performance and problem issues.

The County System will deploy remote system management software on a 24 x 7 basis. This RMS application software will provide real-time monitoring of the MBIS and processes providing status as well as active alerts from all server system types back to a centralized repository monitoring center. In addition, this RMS package allows the Contractor-County team the capability to provide a number of different monitoring / diagnostic tools and resources that are used as part of the overall check for System integrity. This application can monitor networked devices, application processes and services, as well as retrieving pertinent System logs, if needed. This package allows the capability to automatically report system or subsystem errors, based upon a problem priority responsive scheme, providing immediate simultaneous notifications to the County office as well as the Contractor-County support team. Common system logs can be automatically retrieved and examined to provide engineers with valuable information as to the status of particular device and/or services being run. This RMS application will also work in an offline fashion as a diagnostics tool. The remote monitoring of functions and processes will also play a major role in the review of all automated performance and system audits.

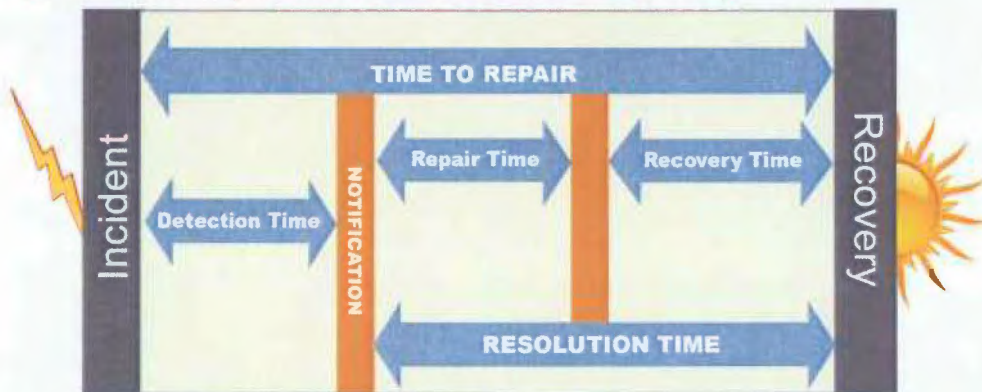
As illustrated in Figure 6, the RMS reduces problem mean-time-to-identification, mean-time-to-notification, mean-time-to-resolution, and network downtime and business risk.

Figure 6: Contractor's RMS Reduces Recovery

Typical Recovery Process



**Contractor's Enhanced Recovery Process
(Elimination of response time and shortened resolution time)**



Contractor will provide the County with direct access at any time to the data collected as a result Response Time monitoring. Whenever requested by County, Contractor will provide the County with reports and/or download that data along with all applicable documentation that may be necessary for the County to independently monitor the Response Time of the System.

Contractor understands that the County reserves the right to periodically revisit the Response Time baselines for resetting to ensure that the Response Time of the Solution does not restrict or delay the County's operations.

PREVENTIVE MAINTENANCE

Preventive Maintenance, or Periodic Maintenance, (PM) for the County MBIS—both networked and direct connect—will be scheduled and performed on a regular basis. Most PM tasks will be performed on a weekly, monthly, quarterly, or semi-annual basis, while the System is still online and operational. Preventive maintenance tasks at the Primary Site System will take approximately six to nine hours, but it is expected that, due to redundant and clustered server configurations, System downtime for the County MBIS Primary Site, Remote Sites, and COOP Site is expected not to exceed two hours in any given month, unless agreed to by the County. Contractor will schedule the services at the Primary Site and COOP Site at alternate times. With prior approval from the County, additional scheduled maintenance will be performed at a downtime with least impact on the County operations. Table 38 details preventive measures.

Table 38: Preventive Maintenance Measures

PREVENTIVE MAINTENANCE MEASURE	
<ul style="list-style-type: none">• Visual inspection of all hardware devices and components• Review of all performance, System backup service, transaction and performance logs including incremental backup for any problem issues• Research stalled transaction jobs, if any• Disk maintenance (hardware and/or software)• Maintaining/Update problem log and site activity/incident report through an automated call collection system, and escalated technical problems through the TFS system (Escalated Problem Tracking System)• Virus detection audit and service required, if any.• Security and anti-virus software updates check for automated rollouts• Run and review System hardware and software performance reports (Remote Monitoring Software tools)	<ul style="list-style-type: none">• Firmware updates and System software patch releases – Subject to approval through the change control process• Database/Queue-file maintenance and disk application logging maintenance• Maintaining proper software versioning, and patch release control methodologies subject to approval and release of the change control process• Adjustment and or realignment of software configuration tables, access lists and replacement of worn or defective parts• Review of automated incremental backups, correct as necessary• Performance of any cold backups, image backups• Performance of Image workstation and Server saves• Repair or replacement of any defective hardware components and subsequent handling of parts replacements

SCHEDULED DOWNTIME

Contractor will provide all Maintenance Services, including installation of Software Updates and Hardware Upgrades, during Scheduled Downtime, during late evening hours or early morning hours in order to avoid times when users need to use the System, as agreed to by the County. Scheduled Downtime for performing Preventive Maintenance or other Maintenance Services at any site shall not exceed two (2) hours for each site in any month, unless agreed to in advance by the County.

Any Downtime outside of the above window of time without prior County approval will be considered Unscheduled Downtime and will entitle the County to remedies as specified in the SLP. Notwithstanding the foregoing, Contractor may request Scheduled Downtime for the provision of an emergency correction to the Solution. Such Downtime will be deemed Scheduled Downtime, provided that it has been approved by the County's Project Manager.

CORRECTIVE MAINTENANCE

Contractor will restore all functions as originally implemented, if there is any deficiency in Contractor provided equipment and software, when used as delivered, if it fails to perform in accordance with the documented technical specifications. This includes the repair, replacement, or exchange of System components and/or software. This service will be provided 24 x 7, 365 days per year for the County Primary, COOP, and Remote Sites. Contractor engineers will make every effort to address the issues as quickly as possible, but always within the timeframes provided in the Service Level Proposal.

Remote diagnostics and Level 2 support will be provided to isolate and further diagnose System or subsystem issues. All problems will be coordinated through the site assigned Contractor engineers. At all times, the County will be kept informed of the System or device status and situation at hand.

For corrective maintenance calls, Contractor may, depending on the issue at hand, use VPN remote access to correct a System or remote workstation issue. This will significantly reduce any downtime which might occur due to travel time. Remote access has proved to be extremely effective and will again significantly reduce downtime experienced by the end user. The majority of service calls can be addressed remotely due to available tools to the engineer on hand.

DEFICIENCY IDENTIFICATION

Problems may be identified as a result of remote monitoring or discovered and reported by the County. All identified problems will be reported, prioritized and resolved.

DEFICIENCY PRIORITY LEVELS

The priority level for each reported deficiency will be assigned based on the Deficiency Priority Level table in the SLP (DEL-33).

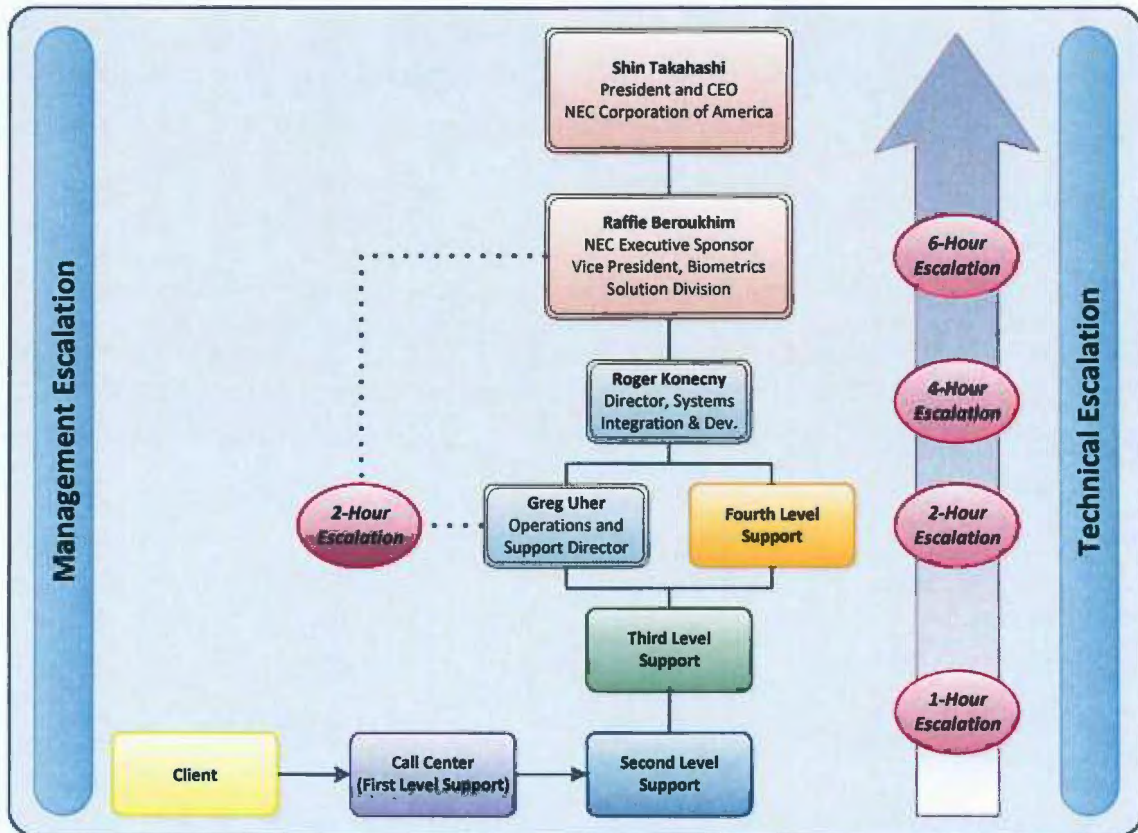
DEFICIENCY RESOLUTION

Contractor will resolve deficiencies per the SLP (DEL-33) and the procedure provided in the following section, "Coverage and Escalation."

COVERAGE AND ESCALATION

Contractor will provide an end to end support service. This support will be provided by local Contractor County-assigned engineers who will provide all hardware and first-level software support. Should second-level support be required, for either hardware or software, the local engineer will immediately escalate to the Level 2 support team in Long Beach, CA. Should third-level support be needed, the Level 2 support engineer will escalate to Level 3 support team in Rancho Cordova, CA. If Level 3 support team is unable to resolve the problem, then the issue will immediately be escalated to the development group, in Rancho Cordova, CA. All Contractor support functions will operate in a 24 x 7, 365 days per year environment. Contractor escalation policy, as depicted in Figure 7, ensures that critical issues are addressed and the senior management is alerted to provide required direction and access to additional resources.

Figure 7: Contractor-County Emergency Call Process and Escalation



Due to the 24 x 7 requirement of County MBIS, secure remote access is required to support the County System. This support allows for a fast, efficient, service for the Primary and Report Sites. Should onsite service be required for any remote, Contractor will provide an onsite in accordance with the County priority level assignments. Every effort will be made to provide remote access support. This will eliminate unwanted or unneeded downtime.

CRITICAL SPARE PARTS – SPARE PARTS PROVISIONING

Spare kits containing critical spare parts for the County MBIS will be the sole responsibility of Contractor and will be defined after System build is completed. In addition, Contractor has a parts depot located in Long Beach and throughout the United States to provide rapid access to required spare parts.

REPAIR / REPLACEMENT OF DEFECTIVE COMPONENTS

Contractor shall keep the MBIS running at its optimal performance. If a component has failed, or has experienced the same problem three (3) or more times during a 30-day timeframe, such as an intermittent problem, the component shall be considered defective and will be repaired or replaced. Contractor assumes sole responsibility for securing the parts, provided the equipment was supplied by Contractor.

All replacement parts are new or refurbished to factory standards. Removed or installed replacement parts become the property of Contractor. Critical spare parts are stocked onsite and at strategic locations around the country. A Contractor site requiring a part that is out of stock locally will quickly receive the part from another site within the region.

Parts are routinely shipped overnight or hand carried. An automated Inventory Control System monitors inventory levels, records parts usage, and alerts logistics personnel when inventories are at a low level. The System provides a high level of visibility and 24-hour access to all spares parts stocked throughout the country.

RECONFIGURATION / SYSTEM MOVES

Occasionally, the County sites have equipment relocation needs. Should this happen, Contractor will work with the County to address the specific situation. A reconfiguration of MBIS Primary Site equipment or transportation of MBIS equipment to a new facility will be scheduled through the County. The County will be responsible for the cost of such reconfiguration or moves at a mutually agreed to price.

VERSION DESCRIPTION DOCUMENTATION

Contractor will maintain a Version Description Document (DEL-26) comprising the complete and detailed instructions necessary for installation (install and configure) for all hardware, software, and data associated with each deployment. This includes site specific information. This information will be cataloged and store on the Contractor operations server in a specific area for the County. The server is backed up on a daily basis and is access restricted for security purposes.

TECHNICAL COORDINATION WITH NETWORK SUPPORT

As part of the support package, Contractor will provide ongoing cooperative support to assist with any technical network issues as well as security configurations which could possibly affect the performance of the County MBIS. This coordination will be in support of the County administrative, staff, and Remote IT department staff. Contractor maintains that working together to resolve a System network issue is the quickest way to correct the problem. Contractor will also provide periodic reporting of routine activities, problems/issues, and resolution status.

LEVELS OF SERVICE

Please refer to the Service Level Proposal (SLP, DEL-33).

RISKS

Table 39: Maintenance Services Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Hardware may become end of life during the life of the contract, making the sourcing of replacement parts difficult.	Contractor will maintain spare parts in our warehouses and evaluate and provide next model level delivery, when appropriate. An example of this policy is that a failed hard drive may be replaced with a model from a different manufacturer at a higher specification than the original.

APPLICABLE STANDARDS

Contractor will adhere to all agreed upon standards set for levels of service and support. We will meet with LASD on a mutually defined rotation to discuss the metrics for measuring these standards.

Contractor is a process driven, policy oriented vendor. Our comprehensive policies govern such activities as:

- Access to customer networks only by security cleared personnel
- Information Security, ensuring the safeguarding of customer data and the use of anti-virus software
- Physical Security of our data centers and networks

For System Support, the most visible policy is adherence to CJIS Security Policy version 5.2. All Contractor staff shall undergo fingerprint based background checks at the State and Federal levels. Prior to beginning work on a project, staff are also required to attend the requisite CJIS training provided by our on-staff CJIS Security Officer (CSO).

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- Service performance at or above the agreed levels. We will support the System on a 7 x 24 schedule and meet the System uptime requirements.
- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes
- **DEL-33:** Service Level Plan
- **DEL-10:** In-Plant Security Plan.

SECTION 3.4.1 TECHNOLOGY REFRESH AND ENHANCEMENTS

As part of Maintenance Services, Contractor shall propose functional and processing requirements for, and implement, future upgrades. Contractor shall also identify and make recommendations concerning the operation of the Existing System, including but not limited to ensuring that the Service Levels are maintained and that Contractor is performing other duties as agreed to by County and Contractor under the Agreement.

Contractor and County shall conduct periodic joint technology reviews, no less frequently than every six (6) months, to guarantee that the hardware and software are adequate for County purposes and are consistent with then-current technology used in similar systems. Such evaluations shall include reviewing the available technology applicable to the MBIS, both from Contractor and third parties, and reviewing pending and implemented changes in NIST, EBTS and other standards applicable to County or its Remote Sites. As may be required from time to time, Contractor and County shall determine any hardware or software changes that are needed to respond to such developments and to provide migration paths for such functional or technology updates. Such changes shall be provided at no cost to County beyond the Service Fees payable by County to Contractor.

As part of Maintenance Services, Contractor shall provide at least two (2) hardware refreshes during the entire term of the Agreement at no additional charge to County beyond the Service Fees. Prior to commencing hardware refresh, Contractor shall submit for County approval technology refreshment specifications, which shall incorporate technological upgrades that are Necessary to maintain MBIS performance at the requisite Service Levels and to improve such performance, including through additional functionality or in response to changes in technology, regulations or standards applicable to law enforcement promulgated by CalDOJ, the FBI or Department of Homeland Security. Contractor shall furnish agendas, presentation materials, minutes and technical reports.

Contractor will comply with the technology refresh and enhancement requirements of Section 3.4.1, Section 3.4.2, and Section 3.4.3 of the SOW.

This section describes Contractor's approach to satisfying the technology refresh and enhancement requirements of the SOW. Described below is Contractor's approach for maintaining an awareness of the state of the art in biometrics and other relevant technologies; and for identifying and evaluating new commercial software products and product upgrades for insertion into the MBIS baseline.

CONTRACTOR'S SOFTWARE RELEASE POLICY

Contractor's software release policy follows an industry standard process.

The main activities involved in Release Management are:

- Establishing a planning policy for the implementation of new versions.
- Developing new versions
- Testing new versions in an environment that simulates the live environment as closely as possible.
- Validating the new versions.
- Implementing new versions in the live environment.
- Version control

The software release version is identified by three numbers. For example, in software release 4.6.1:

- 4 reflects a version of a major release of software,
- 6 reflects a version of a minor release of software
- 1 reflects a version of a supplemental release of software

Contractor's policy for System upgrades is as follows:

- Supplemental releases are defined as releases that materially impact the operational performance or functional performance of the software (patches and bug fixes). LASD and all Contractor customers are entitled to all such releases, on an if and when available basis, without any expense. All expenses for software, hardware, and professional services required for installation of such Releases, assuming customer has a maintenance and support agreement with Contractor, will be covered by Contractor.

- Minor Releases or Enhancements are defined as releases that improve or augment the utility, efficiency, performance, or functional capability of the software. LASD and Contractor customers are entitled to receive this software release free of charge, on an if and when available basis, again assuming a maintenance policy is in effect. Any additional hardware and professional services required for installation of Minor Releases are the responsibility of the customer.
- Major Releases defined as releases that in whole or part introduce new advances in technology. Major releases reflect significant improvements in the product for which the customer is responsible for all hardware, software, and professional services required for implementation of the release.

APPROACH

Contractor understands the County's requirements and will work with the County to identify and make recommendations concerning the operation of the MBIS, including but not limited to ensuring contracted service level is maintained and Contractor is performing the duties as mutually agreed to by the County and Contractor. Contractor complies with the requirements for technology refreshment and enhancement set forth in Section 3.4.1 – Technology Refresh and Enhancements of the SOW.

Contractor plans to review the upcoming System requirements with the County during the bi-annual Joint Technology Review meetings. Based on these discussions, Contractor will review the current System configuration and determine potential hardware or software refreshment items required to meet the agreed upon Service Level Plan.

Contractor's configuration management goals are to manage the complex process of the periodic updates of application, changes in operating systems, security, and obsolescence of hardware with minimum interruption of operations. Contractor's configuration management methodology described in Section 3.6 will handle the additional challenge of maintaining and updating multiple locations and devices.

The development and maintenance of the MBIS System by the Contractor North America Biometric Center of Excellence (COE) will help to manage the consolidation of incremental changes in functionality, defect resolution, and compatibility changes. Contractor's COE is responsible for the technology roadmap. The releases of software on a periodic basis to the Primary, COOP, and Remote sites will be critical and validated by Contractor operations personnel as part of the Configuration Management Plan (DEL-29).

Contractor's System hardware replacement strategy is designed to ensure the MBIS will at a minimum meet the System performance requirements, while ensuring all hardware and associated operating systems are fully supported. During years 2 through 5 of the contract, Contractor plans to review the current System hardware capabilities and upcoming System requirements with the County during the Joint Technology Review meetings. Based on these discussions, Contractor will incrementally add additional matching hardware as required to meet the agreed upon service and performance levels. In addition, Contractor will replace the following hardware:

- Contractor provided MBIS workstations and associated peripherals in Year 4 of the initial 6-year contract term.
- System SAN Storage at both the Primary and COOP site in Year 5 of the initial 6-year contract term.

- Matching server components at both the Primary and COOP site in Year 1 of the extended 4-year contract term.

ASSUMPTIONS

Contractor has made the following assumptions as part of our technology refreshment strategy:

- The System yearly growth and throughput rates will not exceed the 2% estimation provided by the County.
- They System throughput and response times will not exceed the specifications provided by the County.

RISKS

Table 40: Technology Refresh and enhancement Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Hardware/Software end of manufacturer support.	Contractor understands that third part supplied hardware and software products reach a point at which they are no longer supported by the manufacturer. As the end of support is usually well documented, Contractor will review components that are approaching end of support with the County during the bi-annual Joint Technology Review sessions and determine the technology refresh path to ensure continued product support.
Hardware component failure and replacement parts availability	As hardware systems age individual system components may on occasion fail and need to be replaced. Contractor has implemented a multi-level process to ensure hardware component failure does not impact system performance. All hardware components within the system are deployed with fully redundant configurations. Contractor stores and maintains an internal parts inventory for full replacement of workstations and printers. Contractor procures all hardware from well-established vendors that guarantee availability of replacement parts throughout the warranty period.
Changes to local, state, and national standards	Contractor will discuss changes to biometric related standards during the bi-annual Joint Technology Review meetings to determine the impact to LASD operations. Based on these discussions Contractor will determine the MBIS system changes required to comply with the updated standards.

APPLICABLE STANDARDS

- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- Electronic Biometric Transmission Specification (EBTS), NGI-DOC-01078-10.0.
- IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.2, CJIS Security Policy, Version 5.2, dated August 9, 2013.
- California Department of Justice (Cal-DOJ) Live Scan Transmission Standards

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-07:** Agenda
- **DEL-08:** Presentation Materials
- **DEL-09:** Minutes
- **DEL-20:** Technical Report.
- **DEL-29:** Configuration Management Plan (updated as necessary).

SECTION 3.4.2 SOFTWARE UPDATES

Contractor shall provide Software Updates to the Software, on an if and when available basis, to keep current with Contractor's hosting technology standards, industry standards, Third Party Software upgrades, enhancements, updates, patches, bug fixes, etc., the System Requirements and as provided to Contractor's general customer base, all in accordance with this SOW and in coordination with County's Project Manager. By definition, such Software Updates shall include, but not be limited to, enhancements, version releases and other improvements and modifications to the Software, including Application Software.

Maintenance Services additionally include maintaining compatibility of the Solution Software with any and all Interfaces provided by Contractor under this Agreement. Prior to the installation of any Third Party Software, or any update thereto, Contractor shall test and ensure such Third Party Software's compatibility with the then current version of the Software. Contractor shall ensure that the Software is compatible with all required or critical updates to Third Party Software, including without limitation, service and compatibility packs and security patches, promptly upon their release.

Notwithstanding the foregoing, any Third Party Application that may be incorporated by Contractor into the Application Software shall be subject to the same Maintenance Services obligations and requirements as the Application Software components that are owned by, or are proprietary to, Contractor.

SECTION 3.4.3 SYSTEM ENVIRONMENT

As part of Maintenance Services, Contractor shall also provide maintenance of the System Software that is part of the Server Environment for the Solution, including but not limited to operating software, database software and other software installed in the Server Environment that is not Application Software. Contractor shall update, upgrade, replace and/or maintain such System Software components during the term of the Agreement to comply with the System Requirements and the warranties specified in this Agreement and to be compatible with the Application Software, including any Application Modifications provided by Contractor under the Agreement.

Contractor shall provide Software Updates to the System Software to keep current with Contractor's hosting technology standards, industry standards, Software Updates to the Application Software and other Application Modifications, all in coordination with County's Project Manager.

As part of Maintenance Services, Contractor shall also provide maintenance of the Server Hardware components surrounding the Software, including but not limited to all equipment and networking components and other Hardware Upgrades at no additional cost to County beyond the applicable Service Fees. Contractor shall repair, upgrade, replace and/or maintain these System Hardware components during the term of the Agreement to comply with the System Requirements and the warranties specified in this Agreement and to be compatible with the Software including any Application Modifications provided by Contractor under the Agreement.

Furthermore, Contractor shall, during the term of the Agreement, maintain the Solution's compatibility with County's Client Environment by providing, among others, Software Updates to the Software and Hardware Upgrades to the Solution Hardware.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor shall provide the following Deliverable(s) for this component of the SOW:

- **DEL-26:** Version Description Document
- **DEL-33:** Service Level Plan

SECTION 3.4.4 SCHEDULED DOWNTIME AND PREVENTIVE MAINTENANCE

Unless agreed to otherwise in advance by County and Contractor, Contractor shall provide all Maintenance Services, including installation of Software Updates and Hardware Upgrades, during Scheduled Downtime, during late evening hours or early morning hours in order to avoid times when users need to use the System, as agreed to by County. Scheduled Downtime for performing Preventive Maintenance or other Maintenance Services at any site shall not exceed two (2) hours for each site in any month, unless agreed to in advance by County.

Any Downtime outside of the above window of time without prior County approval shall be considered Unscheduled Downtime and shall entitle County to remedies as specified in this SOW. Notwithstanding the foregoing, Contractor may request Scheduled Downtime for the provision of an emergency correction to the Solution. Such Downtime shall be deemed Scheduled Downtime, provided that it has been approved by County's Project Manager.

County and Contractor shall agree on Scheduled Downtime as part of IMS.

Contractor will perform a documented Preventive Maintenance procedure for all equipment and software they provide. Contractor shall periodically dispatch maintenance personnel to clean, inspect and adjust the equipment and replace defective or worn parts thereof at the manufacturer's recommended frequency in order to keep the equipment in good operating condition. Contractor shall carry out periodic maintenance tasks on all electronic components they provide to ensure they are operating at maximum capability. Such maintenance shall be scheduled to be performed, at a minimum, once a month during hours agreed to by County.

Contractor shall provide the following Deliverable(s) for this component of the SOW:

- **DEL-33:** Service Level Plan.

SECTION 3.4.5 RESPONSE TIME MONITORING

Contractor shall be responsible for monitoring Response Time of the System to ensure compliance with the System Requirements including System Performance Requirements set forth in this SOW with all Attachments.

Contractor shall perform Response Time monitoring at regular intervals and in sufficient detail to detect problems. Contractor shall provide County with direct access at any time to the data collected as a result Response Time monitoring. Whenever requested by County, Contractor shall provide County with reports and/or download that data along with all applicable documentation that may be Necessary for County to independently monitor the Response Time of the System.

County reserves the right to periodically revisit the Response Time baselines for resetting to ensure that the Response Time of the Solution does not restrict or delay County's operations.

SECTION 3.5 CORRECTION OF DEFICIENCIES

During the System Operation Phase of the Agreement, as part of System Maintenance, Contractor shall correct the Deficiencies in the System, as further provided in this Section 3.5 – Correction of Deficiencies below.

Contractor shall provide corrective maintenance for any Deficiency in Contractor provided equipment or software that, when used as delivered, fails to perform in accordance with the Specifications specified in the Agreement, including System Requirements. The period for the provision of corrective Maintenance coverage for all hardware and software shall be defined as 24/7.

Contractor shall maintain an electronic report log that indicates the problem report number, problem description, the time that the problem call was received, the priority assigned, all actions taken and the time that the problem was corrected. The problem report log shall be maintained in a database that is remotely accessible by County personnel.

Contractor shall offer one central point of contact for support of hardware and software. Contractor support personnel shall address all problems reported by County's Help Desk staff. Contractor's support personnel shall acknowledge problems reported via telephone or by e-mail within one (1) hour and respond according to the protocols listed below.

SECTION 3.5.1 IDENTIFICATION OF DEFICIENCIES

The Deficiencies under this Agreement may be identified either as a result of Contractor's use of its own monitoring System or discovered by County. Upon discovery of a Deficiency by County, County will report the Deficiency to Contractor's Customer Support for resolution in accordance with this SOW.

The Priority Level of a Deficiency shall be assigned according to the Priority Level definition set forth in Section 3.5.2 – Deficiency Priority Levels. Based on Contractor's proposed solution and/or a workaround for the Deficiency, County may reevaluate and escalate or downgrade the Priority Level of such Deficiency.

SECTION 3.5.2 DEFICIENCY PRIORITY LEVELS

County shall assign the Priority Level to each Deficiency reported by County to Contractor's Customer Support. Contractor shall assign Priority Levels to Deficiencies discovered by its own problem monitoring system. Following report of a Deficiency from County, Contractor shall respond back to County within the prescribed "Response Timeframe" specified below and resolve each such Deficiency within the specified "Resolution Time". Resolution Time for correction of Deficiencies shall start tolling when County first notifies Contractor of a Deficiency by telephone or otherwise as specified herein, including Contractor's Customer Support, and shall end when County determines that the Deficiency has been resolved.

PRIORITY LEVEL	DESCRIPTION OF DEFICIENCY	RESPONSE TIMEFRAME	RESOLUTION TIME
1 – Critical	System is down (Unscheduled Downtime) or is practically down (e.g., extremely slow Response Time) or does not function at all, as determined by County. There is no way to circumvent the problem; a significant number of County users are affected. A production business System is inoperable.	One (1) hour	Eight (8) consecutive hours
2 – Severe	A component of the Solution is not performing in accordance with the Specifications (e.g., slow Response Time), creating significant County business impact, its core functionality is not available or one of System Requirements is not met, as determined by County.	Four (4) hours	Two (2) Business Days
3 – Moderate	A component of the Solution is not performing in accordance with the Specifications; there are unexpected results, moderate or minor operational impact, as determined by County.	One (1) day	Two (2) weeks
4 – Low	This is a low impact problem and is not significant to operations or is related to education (e.g., general "how to" and informational Solution Software questions, Documentation requests, understanding of reports or general "how to" create reports), as determined by County.	Two (2) days	Next version release or six (6) months unless otherwise agreed to by County and Contractor

SECTION 3.5.3 PROBLEM RESOLUTION AND PROTOCOLS

County shall assign the Priority Level to each Deficiency reported by County to Contractor's Customer Support. Contractor shall assign Priority Levels to Deficiencies discovered by its own problem monitoring system. Following report of a Deficiency from County, Contractor shall respond back to County within the prescribed "Response Timeframe" specified below and resolve each such Deficiency within the specified "Resolution Time". Resolution Time for correction of Deficiencies shall start tolling when County first notifies Contractor of a Deficiency by telephone or otherwise as specified herein, including Contractor's Customer Support, and shall end when County determines that the Deficiency has been resolved.

Problems that require an immediate response (Priority Level 1) are System or component failures that prevent subjects from being enrolled, images from being searched or responses from being delivered. This includes all equipment supplied by Contractor associated with the System, including Remote Site printers, scanners and other required peripherals that would prevent users from accomplishing their work.

Contractor may attempt to correct the problem by phone or remote access. If Contractor is unable to correct the problem in this manner, Contractor must begin on-site repair within four (4) hours of the time Contractor was initially notified, depending on the availability of the site where the equipment resides. All situations that prevent the initiation of on-site repair within such four (4) hours will be documented in Contractor's electronic report log and reported to County's Help Desk.

Contractor must ensure that the equipment will be repaired within eight (8) consecutive hours. If a device is out of service for eight (8) consecutive hours from the time Contractor was notified, Contractor shall, by the end of the eighth hour, replace the defective equipment with an operable device until the defective item has been fully repaired. The eight (8) hour clock begins from the time of personal notification to Contractor.

All other Major Deficiencies (Priority Level 2) will be corrected within two (2) Business Days from the time the problem was reported.

Contractor shall inform County within 1 hour of any service interruptions and then notify the County within eight (8) hours of any hardware or software problems that Contractor has identified and resolved.

Contractor shall provide the following Deliverable(s) for this component of the SOW:

- **DEL-33: Service Level Plan.**

SECTION 3.6 CONFIGURATION MANAGEMENT

County's Remote Sites are geographically dispersed over a large area. This dispersion poses unique problems related to problem reporting, testing, diagnosis, deployment of patches and revisions and other aspects of configuration management. Configuration management plans and processes must address these unique problems efficiently and effectively.

Contractor shall document and implement a Configuration Management Plan [DEL-29] and processes that shall address these unique problems efficiently and effectively. Configuration management performed by Contractor shall accomplish the following:

- Establish a controlled configuration for each operational hardware and software component at the Primary Site, the COOP Site and each Remote Site
- Maintain current copies of the deliverable documentation and code
- Give County access to the documentation and code under configuration control
- Control the preparation and dissemination of changes to the master copies of the delivered software and documentation placed under configuration control so that they reflect only approved changes.

Contractor shall generate management records and status reports for all hardware and software products at the Primary Site, the COOP Site and each Remote Site, including the controlled operational configurations. The status reports shall:

- Make changes to controlled products traceable
- Serve as a basis for communicating the status of configuration identification software and associated software
- Serve as a vehicle for ensuring that delivered documents describe and represent the associated software.

Contractor shall participate in County configuration control meetings. County configuration control meetings will establish and control the requirements baseline [DEL-02] throughout the performance of the Agreement and will control the operational baseline, including deployed hardware, software, databases and documentation, once the MBIS becomes operational.

Contractor will comply with the configuration management requirements of Section 3.6 – Configuration Management of the SOW.

This section describes Contractor's approach to satisfying the configuration management requirements, including any risks, applicable standards, deliverables and deliverable content.

APPROACH

Contractor understands the complexities involved with administering and maintaining geographically dispersed systems. Contractor has the experience of handling successfully, many MBIS implementations, which feature remote workstations, that are not only geographically remote, but often, have limited bandwidth connections to the Primary site. To address these challenges we have designed our architecture to centralize the software deployment and rollout.

In addition to the System architecture design, we utilize several commercially available tools to help us manage the System configuration. For Windows server, and workstation configuration and deployment we utilize Microsoft System Center Configuration Manager (SCCM). This allows for centralized automated control of the application versions and deployment. In addition for defect tracking, task management, code source control, builds, and release management we utilize Microsoft's Team Foundation Server (TFS) as an application life cycle management platform. The tools and methods being used allow Contractor to establish and maintain controlled configurations for the hardware and software components at the Primary Site, COOP Site, and Remote Sites. The unique problems due to the County's geographic dispersion are addressed using these tools.

Throughout the life of the contract Contractor will provide a comprehensive configuration management documents that will adhere to the County's deliverables and requirements.

A Preliminary Configuration Management Plan (**DEL-29**) is attached with the Business Proposal. This plan details how we meet the County's configuration management goals of:

- Establishing a controlled configuration for each operational hardware and software component at the Primary Site, the COOP Site and each Remote Site.
- Maintaining current copies of the deliverable documentation and code.
- Giving the County access to the documentation and code under configuration control.
- Controlling the preparation and dissemination of changes to the master copies of the delivered software and documentation placed under configuration control so that they reflect only approved changes.

Additionally, Site Installation Reports which specifically detail the following information will be prepared for the Primary, COOP, and each of the local agency sites:

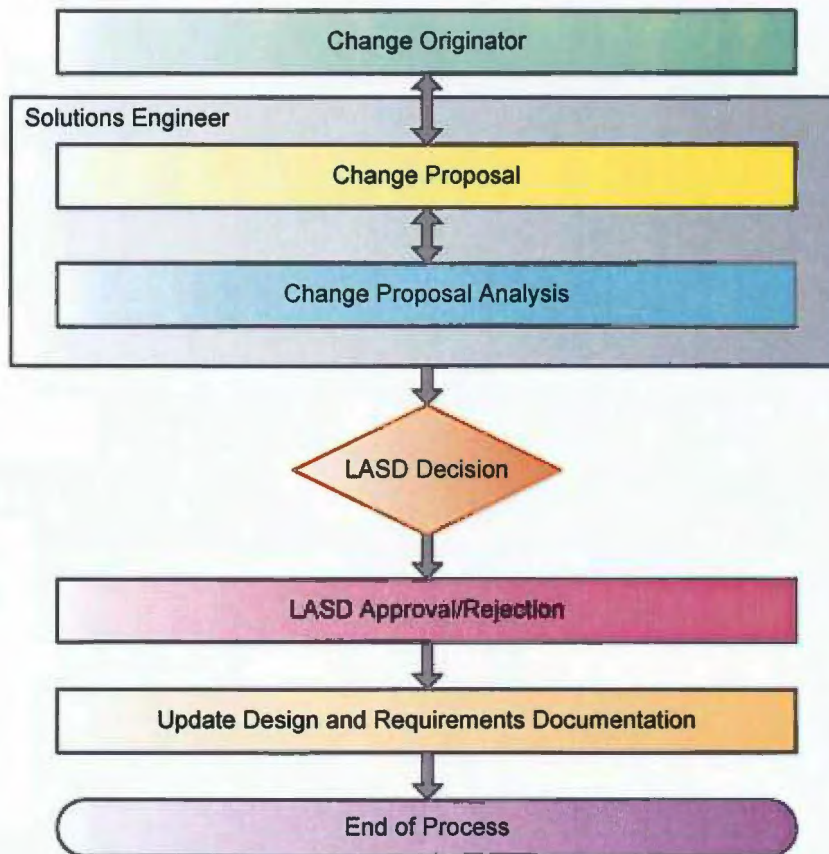
- Installed hardware
- Network connections
- Assigned IP addresses
- Current operating systems
- Installed middleware
- Installed Contractor software including details the currently installed release versions
- Diagrams showing hardware connections and locations

These Site Installation reports will be maintained and updated as the site configuration changes. These Contractor standard implementation documents, with their included change tracking, will meet the county's requirement for management and status reports regarding configuration control.

Finally, Contractor will prepare a Version Description Document (**DEL-26**) detailing all deployment and installation instructions for all System components. This allows for full rebuild of the System solely from the description document.

Contractor will be an active participant in the County Configuration Control meetings throughout the implementation of this project and subsequently once the MBIS is operational. Figure 8 provides an overview of Contractor's standard configuration proposal process.

Figure 8: Configuration Change Proposal Process



RISKS

Table 41: Configuration Management Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Availability of Source Code	Contractor utilizes a centralized source code repository (TFS) that maintains all versions and change history of the code under management. In addition this repository is backed up nightly to ensure all original source code is fully available even in the event of a disaster situation
User installed Applications	By using a centralized system control management platform (SCCM) and directory system, Contractor administrators can control user rights, and control system deployments.
Unforeseen impacts of change requests	Contractor follows a complete change control management process which includes multi-level review of all proposed changes. This helps to identify potential conflicts and raise issues prior to requirements finalization.

APPLICABLE STANDARDS

- IEEE Standard 1058, Software Project Management Plans, Configuration Management Plan
- IEEE Standard 828, Software Configuration Management Plans
- ISO 10007, Quality Management – Guidelines for Configuration Management
- EIA649, National Consensus Standard for Configuration Management

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-02:** System Requirements Specifications
- **DEL-26:** Version Description Document
- **DEL-29:** Configuration Management Plan.

SECTION 3.7 CONTINUITY OF OPERATIONS

As part of System Maintenance, Contractor shall also be responsible for the provision of COOP Services in accordance with the COOP Plan provided by Contractor in accordance with this SOW.

Contractor or County may declare an event a Disaster. As part of COOP Services, Contractor shall perform the functions; provide or utilize the facilities, equipment, supplies, data, and documentation; and conduct the training and exercises/drills specified in the COOP to maintain a viable COOP capability that ensures the performance of Contractor's essential functions during any emergency or situation that may disrupt normal operations and leave Contractor facilities damaged or inaccessible. Contractor shall be subject to the following Service Level Requirements as part of COOP, which shall be contained in and are incorporated into the COOP Plan:

- Contractor shall have complete responsibility for restoration of the Solution.
- In the event of a Disaster declaration, Contractor shall be required to maintain regular and consistent communication with County about the outage and steps taken to restore the Solution.
- Contractor shall be required to make a declaration of a Disaster and invoke the Disaster Recovery Plan within twelve (12) hours from the disruption of the Operational Environment or precipitating event.
- Contractor shall restore the System Data to a point no greater than twenty-four (24) hours prior to the declaration of the Disaster by County or Contractor.
- County shall be able to logon to the Disaster Recovery site within forty-eight (48) hours of the declaration of the Disaster by County or Contractor.
- Contractor shall have at a minimum 50% capacity within forty-eight (48) hours and 100% capacity within ninety-six (96) hours of the declaration of the Disaster by County or Contractor.
- Contractor's failure to make a declaration of a Disaster within twelve (12) hours shall result in the incident and deemed Unscheduled Downtime.

Contractor will comply with the Continuity of Operations (COOP) requirements of Section 3.7 – Continuity of Operations of the SOW. This section describes Contractor’s approach to satisfying the COOP requirements, including levels of service, assumptions, risks, applicable standards, deliverables and deliverable content.

APPROACH

The County MBIS serves a mission critical purpose and, as such, is in need of an emergency action plan in case of a catastrophic event. To ensure the successful execution of these mission-essential functions and to maintain MBIS services for the law enforcement communities they serve, Contractor will actively participate in the COOP planning and implementation.

Contractor fully complies with the requirements for Continuity of Operations outlined in the SOW and details of the COOP and associated implementation plan are provided in the Continuity of Operations Plan deliverable (DEL-22). Contractor will perform the functions; provide or use the facilities, equipment, supplies, data, and documentation; and conduct the training and exercises/drills specified in the COOP to maintain a viable continuity of operations capability that ensures the performance of Contractor’s essential functions during any emergency or situation that may disrupt normal operations and leave the County’s primary facilities damaged or inaccessible. Contractor is committed to maintaining this System and its functionality throughout the life of the contract and will submit an update to the COOP (DEL-22) for County approval whenever an upgrade is made to the operational County MBIS.

System equipment at the COOP Site will be of the same capabilities as the System in the Primary Site. It will provide for the same functionality, transaction throughput, and storage commitment level.

The COOP Site will be located at the secure facility in Rancho Cordova, CA—which meets all the CJIS security guidelines—and is geographically capable of supporting operations in a threat-free environment. This facility is secure; has sufficient space to perform essential functions; has qualified technical resources; and reliable logistical support, services, and infrastructure systems.

LEVELS OF SERVICE

The levels of service defined by the County are outline in Table 42.

Table 42: Levels of Service

SERVICE	REQUIRED SERVICE LEVELS
Declaration of a Disaster and invoke the Disaster Recovery Plan	Within 12 Hours of disruption of service
RPO (Recovery Point Objective)	Within 24 Hours of disruption of service
Restoration of services – 50% throughput capacity (RTO – Recovery Time Objective)	Within 48 Hours of disruption of service
Restoration of services – 100% throughput capacity	Within 96 hours of disruption of service

Contractor's solution is designed to be Active-Active with both the Primary and COOP sites providing 100% transaction processing capacity. Hence the time required to completely failover to one site in case of a catastrophic event is minimal and is well within the service levels outlined by LASD.

ASSUMPTIONS

In designing the COOP, Contractor assumes that there will be sufficient network bandwidth between the Primary and COOP Sites. It is anticipated that database synchronization processes will be the dominant network traffic activity. Since approximately 20% (or more) of all daily transaction workload occurs during peak hours, it is possible that the hourly data size to be replicated to the alternate database will exceed the WAN connection bandwidth. Thus, depending on the available network bandwidth and peak hour workload, there may be a time lag in database synchronization.

RISKS

Table 43: COOP Planning Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Insufficient network bandwidth between the Primary and COOP sites can cause a lag in data synchronization. In such cases, the recovery point in the event of failure might be greater than zero.	Work with the county during System Design Review and yearly and bi-annual Joint Technology Review meeting to ensure network bandwidth is sufficient for full System processing and synchronization activities.

APPLICABLE STANDARDS

Contractor's disaster handling and recovery procedures based on ISO/IEC 24762:2008.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- o **DEL-22:** COOP Plan.

SECTION 4 REMEDIES

Contractor shall provide the remedies set forth in this section.

SECTION 4.1 SERVICE CREDITS

Credits shall accrue for Unscheduled Downtime, including Contractor's failure to meet the Service Availability requirements and/or Response Time requirements (hereinafter "Service Credit(s)"). For purposes of assessing Service Credits and this SOW, "Unscheduled Downtime" shall mean the total amount of time during any calendar month, measured in minutes, during which the System has a Major Deficiency that is unresolved by Contractor, excluding Scheduled Downtime.

Without limiting any other rights and remedies available to County, either pursuant to this Agreement, by law or in equity, County shall be entitled to Service Credits calculated based on the length of Unscheduled Downtime as provided in the table below. Service Credits will not be assessed for Scheduled Downtime.

LENGTH OF CONTINUOUS UNSCHEDULED DOWNTIME	SERVICE CREDITS
1 to 4 hours	1 day of Service Credits equal to 1/30th of Monthly Fees
Over 4 up to 48 hours	2 days of Service Credits equal to 1/15th of Monthly Fees
Over 48 up to 96 hours	5 days of Service Credits equal to 1/6th of Monthly Fees
Each additional block of 96 hours thereafter	Additional 5 days of Service Credits equal to 1/6th of Monthly Fees

Service Credits shall be calculated separately for each applicable incident of a Deficiency and shall be added up to be assessed at the end of each Service Fee cycle (quarterly). Service Credits, in any amounts, are not and shall not be construed as penalties and, when assessed, will be deducted from County's payment due to Contractor. The total of all Service Credits assessed during any Service Fee cycle will not exceed 10% of the undiscounted Service Fees payment for the applicable Service Fee cycle, provided, however, that any Service Credits in excess of the 10% cap for the particular Service Fee cycle will roll forward and be applied as Service Credits to the Service Fees of the following Service Fee cycle. In no event shall Service Credits for any one-year Maintenance Period exceed 10% of the Annual Fees for that Maintenance Period.

SECTION 4.2 SYSTEM RESPONSE TIME DEFICIENCIES

A Response Time Deficiency that fits the definition of a Major Deficiency as a Priority Level 1 or Priority Level 2 shall be deemed to cause Unscheduled Downtime and shall entitle County to assess Service Credits as provided in Section 4.1 – Service Credits above. In addition, the System shall be deemed to be experiencing Unscheduled Downtime after thirty (30) days of any Response Time Deficiency unresolved by Contractor, entitling County to assess Service Credits.

Contractor will comply with the remedies requirements of Section 4 – Remedies of the SOW.

This section describes Contractor's approach to satisfying these requirements, including levels of service, any assumptions, risks, or constraints, applicable standards, deliverables, and descriptions of deliverable content.

APPROACH

The Service Level Proposal (SLP, **DEL-33**) describes Contractor's approach to satisfying the remedies requirements of the SOW. Any Downtime outside of the Scheduled Downtime window without prior County approval will be considered Unscheduled Downtime and will entitle the County to remedies.

Credits shall accrue for Unscheduled Downtime, including Contractor's failure to meet the Service Availability requirements and/or Response Time requirements (hereinafter "Service Credit(s)"). For purposes of assessing Service Credits and this SOW, "Unscheduled Downtime" shall mean the total amount of time during any calendar month, measured in minutes, during which the System has a Major Deficiency that is unresolved by Contractor, excluding Scheduled Downtime.

Without limiting any other rights and remedies available to the County, either pursuant to this Agreement, by law or in equity, County shall be entitled to Service Credits calculated

based on the length of Unscheduled Downtime as provided in the SLP. Service Credits will not be assessed for Scheduled Downtime.

Service Credits shall be calculated separately for each applicable incident of a Deficiency and shall be added up to be assessed at the end of each month of System Maintenance. Service Credits, in any amounts, are not and shall not be construed as penalties and, when assessed, will be deducted from the County's payment due to Contractor.

Contractor understands that Response Time Deficiency that fits the definition of a Major Deficiency as a Priority Level 1 or Priority Level 2 shall be deemed to cause Unscheduled Downtime and shall entitle the County to assess Service Credits. In addition, the System shall be deemed to be experiencing Unscheduled Downtime after thirty (30) days of any Response Time Deficiency unresolved by Contractor, entitling the County to assess Service Credits.

LEVELS OF SERVICE

Please refer to the Service Level Plan (SLP, DEL-33).

ASSUMPTIONS

Contractor assumes that all credits will be applied to the monthly maintenance payments.

RISKS

Table 44: Remedies Risks and Mitigation Strategies

RISKS	MITIGATION STRATEGIES
Contractor understands that, in the event parts are not available or adequate to repair the equipment, credits can be applied.	Contractor will perform a periodic inventory of the MBIS parts stored at our Long Beach part depot, to ensure adequate supply.

DELIVERABLES AND DELIVERABLE CONTENT

Contractor will provide the following deliverables:

- **DEL-33: Service Level Plan**

ATTACHMENT A.1 – SYSTEM REQUIREMENTS

ATTACHED TO THE SOW

ATTACHMENT A.2 – PROJECT DELIVERABLES

During the System Implementation Phase of the Agreement, Contractor shall deliver those Deliverables identified and listed in the Deliverable Table below. All Deliverables shall be subject to County approval and Acceptance in order to satisfy the terms and conditions of the Agreement.

During the System Operation Phase of the project, Contractor shall provide County and its Remote Sites with a comprehensive set of user, System, training and management documentation. Contractor shall supply documentation in both electronic and hard-copy formats. User documentation shall describe the components, functions and operations of each workstation type. Each MBIS workstation shall be provided with online user documentation that is resident on the workstation or accessible via the agency's internal networks.

In addition, Contractor shall deliver those items identified in the table below.

Table 45: Project Deliverables

DOCUMENT No.	DELIVERABLE/PLAN TITLE	DELIVERY DATES
DEL-01	Project Management Plan	With proposal and with update – within 30 days after the Effective Date of the Agreement.
DEL-02	System Requirements Specifications	At System Requirements Review.
DEL-03	Integrated Master Schedule	With proposal and with update at Project Management Reviews.
DEL-04	Test and Evaluation Master Plan	With proposal and with update – within 30 days after the Effective Date of the Agreement.
DEL-05	Migration Plan	At System Design Review.
DEL-06	Test Report – several sets, each corresponding to the outcomes of Factory Acceptance Test, System Acceptance Test and User Acceptance Test	For each increment, at Pre-Ship Review and Operational Readiness Review.
DEL-07	Agenda	Five (5) Business Days prior to a meeting.
DEL-08	Presentation Materials	Draft – five (5) Business Days prior to a meeting, with updates – at the meeting and final – as part of DEL-09.

DOCUMENT No.	DELIVERABLE/PLAN TITLE	DELIVERY DATES
DEL-09	Minutes	Draft – two (2) Business Days after the meeting, with final – five (5) Business days after receipt of County comments.
DEL-10	In-Plant Security Plan	With proposal and with update – within 30 days after the Effective Date of the Agreement.
DEL-11	User Manuals	At each training session and for online reference.
DEL-12	Database Design Document	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and Final as part of DEL-09.
DEL-13	Interface Design Document	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of DEL-09.
DEL-14	System Design Document	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of DEL-09.
DEL-15	Bill of Materials	At System Design Review with updates – at Pre-Ship Review.
DEL-16	Installation Plan	For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review.
DEL-17	Training Plan	At System Design Review with updates – at Pre-Ship Review.
DEL-18	Installation Drawings	At System Design Review with updates – at Pre-Ship Review.
DEL-19	Training Materials	For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review.

DOCUMENT No.	DELIVERABLE/PLAN TITLE	DELIVERY DATES
DEL-20	Technical Report	As specified in Section 3.3.2 – Management and Technical Reporting and Reviews and Section 3.4.1 – Technology Refresh and Enhancements above or as required or requested by County.
DEL-21	Test Procedures	Draft – 30 working days prior to Product Test and Readiness Review and System Test and Readiness Review, with updates – at the review, and final – as part of DEL-09.
DEL-22	COOP Plan	At System Design Review with revision – at Pre-Ship Review.
DEL-23	System Hardware	Prior to Operational Readiness Review.
DEL-24	Software Licenses	Prior to Operational Readiness Review.
DEL-25	System Data	Prior to Operational Readiness Review.
DEL-26	Version Description Document	At Pre-Ship Review with updates – at Operational Readiness Review and Final Acceptance Review.
DEL-27	Installation Survey Report	At completion of each site survey.
DEL-28	Test Plan	At System Design Review with revision – at Test Readiness Review.
DEL-29	Configuration Management Plan	Within 30 days after the Effective Date of the Agreement.
DEL-30	Requirements Verification and Traceability Matrix	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of DEL-09.
DEL-31	System Performance Report	Periodic logs of all transaction and System activity Necessary to evaluate Agreement performance and to facilitate trend analysis, support system and other transactional analysis as specified in Phase 2 of the SOW.

DOCUMENT No.	DELIVERABLE/PLAN TITLE	DELIVERY DATES
DEL-32	Data and Property Management Plan	Contractor shall develop, document and implement comprehensive procedures for the management of data, documentation and County property (equipment, hardware or software that belongs to County).
DEL-33	Service Level Plan	Contractor shall develop a Service Level Plan ("SLP") that will govern the MBIS and Contractor's performance during the System Operation Phase of the project, as outlined in Section 3 – System Operation of the SOW, which shall include all Service Level Requirements set forth in such Section 3 – System Operation of the SOW, Attachment A.3 – Performance Requirements to the SOW and any other requirements specified elsewhere in the Agreement. The SLP must also report performance through DEL-31 above.

ATTACHMENT A.3 – PERFORMANCE REQUIREMENTS

In response to the RFP, Contractor shall submit as part of its proposal a Service Level Proposal, which shall, at a minimum, account for and satisfy all of the Service Level Requirements listed by category below. Contractor's Service Level Proposal shall serve as the basis for the Service Level Plan, to be provided by Contractor in accordance with the SOW, which shall meet all Service Level Requirements, including those set forth in Section 3 – System Operation of the SOW.

SECTION 1 STORAGE CAPACITY REQUIREMENTS

Storage capacities are relevant to the following areas of the MBIS System architecture, including:

- ANSI/NIST Archive
- The templates/features loaded in the matchers

The following under this Section 1 – Storage Capacity Requirements delineate these requirements and will refer to the tables provided below.

SECTION 1.1 ANNUAL SYSTEM MATRIX

Table 46: System Matrix

RECORD TYPE	2009	2010	2011	2012	GROWTH RATE
Registered MAIN Numbers	3,896,801	4,021,159	4,141,491	4,234,079	2%
Records in NIST Archive	3,480,469	3,859,862	4,223,479	4,588,630	2%
Tenprint Searches	408,685	451,997	369,497	357,941	2%

SECTION 1.2 CURRENT LACRIS RECORD COUNTS

Table 47: Record Counts

LACRIS RECORD TYPE	OCTOBER 2012	JANUARY 2013
Tenprints	11,740,616	11,885,223
MAIN Subjects	4,336,089	4,372,098
Palm Prints	N/A	2,257,182
Unsolved Latent	233,882	240,025
Unsolved Palm Latent	92,137	95,580

The MBIS will be designed to accommodate an ANSI/NIST Archive of all input and output transactions through the term of the Agreement. The addition of response TOTs will make the capacity requirements larger than the storage of input transactions only. Most response transactions generated by the MBIS are smaller than the corresponding input transactions. The vendor will have to perform the appropriate design analysis to determine the design requirements in terms of terabytes as a function of transaction type using the data specified in this document.

At the initial operating point of the MBIS, all existing records will have been loaded into the MBIS, including into the ANSI/NIST Archive, the matchers, any other repositories and the master index.

SECTION 2 SYSTEM PERFORMANCE REQUIREMENTS

The MBIS must meet the Performance Requirements (throughput and Response Time) as specified in this Section 2 – System Performance Requirements. The MBIS throughput rates will grow over the life of the System. The following table projects the growth for the Existing Agreement.

SECTION 2.1 ANNUAL LACRIS TRANSACTION COUNTS

Table 48: Transaction Counts

TRANSACTION TYPE	2010	2011	2012	GROWTH RATE
CRM	373,436	350,924	327,197	2%
CUS	0	0	0	2%
REG	5,085	6,427	8,840	2%
SUP	0	0	0	0
COR	0	0	0	0
IDN	41,137	23,444	12,646	2%
IDN2	916	0	0	2%
IDN4	306,073	392,822	339,629	10%
APP	1	1	0	2%
Latent	44,289	54,179	58,737	2%
Palm Latent	18,023	27,803	29,023	2%
TLI	<u>382,409</u>	<u>363,730</u>	<u>345,118</u>	2%
TOTAL	1,171,369	1,219,330	1,121,190	

Legend:

- CRM – criminal booking
- CUS – custody TOT, this is for the inmate realignment. State prisoners being moved to counties
- REG – registrant TOT
- SUP – supplemental
- COR – coroner, deceased
- IDN – identification transaction, state transaction, full roll
- IDN2 – county ID transaction, two index fingers
- IDN4 – county ID transaction, flats (four finger and thumbs)
- APP – applicant (not retained in our AFIS, passed through to DOJ)
- Latent – latent search
- Palm Latent – palm latent
- TLI – tenprint to latent ID.

SECTION 3 RESPONSE TIME REQUIREMENTS

The Response Time for MBIS transactions is a function of the transaction type (identification, forensic, and tactical (Mobile ID)). The Response Times do not include any human interaction times.

The table below provides the Response Times per class of transaction, while the Response Time Requirements table defines the requirements for providing these Response Times.

SECTION 3.1 RESPONSE TIMES PER TRANSACTION TYPE

Table 49: Response Times Per Transaction Type

TRANSACTION CLASS TYPES	RESPONSE REQUIREMENTS UNDER PEAK LOAD
Criminal TP-TP	1 minute
TP-LT	1 minute
LT-TP	1 minute
Palm LT-KP	10 minutes
Criminal KP-LT	5 minutes
Mobile ID TP-TP	30 seconds

SECTION 4 ACCURACY REQUIREMENTS

The matcher accuracy will vary as a function of the class of service (identification, forensic and tactical (Mobile ID)) and the quality of the input images. Identification service accuracy requirements are typically higher than those for forensic services, as the input images are typically of better quality for Live-Scan enrollments than for latent lifts.

Accuracy terms-of-art have been undergoing an evolutionary change for the past few years. While reliability, true accept rate, false reject rate and other terms are often used for access control systems and other biometric modalities (such as facial recognition), a consensus has developed in the international standards community around the terms **true match rate** and **failure to match rate** when discussing friction ridge matching on a large scale.

For this project accuracy will include three (3) accuracy terms:

- **True Match Rate** – the probability that a true match will be found when it is in the background reference file (also known as a repository). This term replaces older terminology such as matcher reliability or true accept rate.
- **Failure to Match Rate** – the probability that a search will not return a true match when the true match is in the reference file. The failure to match rate is 100 percent minus the true match rate. While not explicitly stated in the requirements, it will be calculated during testing and reported.
- **Selectivity** – the number of candidates that will be examined to determine the true match rate. While the system administrators will be able to selectively change the length of candidate lists by transaction class, and by threshold scores, during testing, System accuracy will be measured using the selectivity numbers shown in the table that follows.

SECTION 4.1 ACCURACY RATES BY TRANSACTION TYPE

Table 50: Accuracy Rates by Transaction Type

TRANSACTION TYPES	SELECTIVITY	TRUE MATCH RATE
TP-TP	1	99.9%
Mobile ID TP-TP (with fewer than 10 prints)	8	99.9%
TP-LT	10/25	93%/100%
Criminal KP-LT	10/25	93%/100%
LT-TP	10/25	93%/100%
Palm LT-KP	10/25	93%/100%

SECTION 5 ACCURACY VERIFICATION REQUIREMENTS AND MEASURES

SECTION 5.1 LIGHTS OUT ACCURACY VERIFICATION CONDITIONS

Table 51: Lights Out Accuracy Verification Conditions

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Search Records	10,000	10,000	200	5,000	100
Mated Records	50%	100	100	10	40
NFIQ Average of Mated TPs	3.1 or Better	3.1 or Better	3.1 or Better	N/A	N/A
Minimum Number of Simultaneous Minutiae of Mated Items	N/A	16	16	16	16
Selectivity ¹	1	10/25	10/25	10/25	10/25
True Match Rate ²	99.8%	45%/60%	45%/60%	45%/60%	45%/60%
Non-Mated Search Records	50%	9,900	100	4,990	60
Background Repository	All Converted TP Records	All Converted LT Records	All Converted TP Records	All Converted Palm LT Records	All Converted KP Records

1. Selectivity is a measure of allowed candidate list length.
2. Assumes a true match is in the searched file.

SECTION 5.2 BEST PRACTICES VERIFICATION CONDITIONS

Table 52: Best Practices Verification Conditions

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Search Records	10,000	10,000	200	5,000	100
Mated Records	50%	100	100	10	40
NFIQ Average of Mated TPs	1	1	1	N/A	N/A

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Minimum Number of Simultaneous Minutiae of Mated Items	N/A	12	12	12	12
Selectivity	1	10/25	10/25	10/25	10/25
True Match Rate	99.9%	93%/100%	93%/100%	93%/100%	93%/100%
Non-Mated Search Records	50%	9,900	100	4,990	60
Background Repository	All Converted TP Records	All Converted LT Records	All Converted TP Records	All Converted Palm LT Records	All Converted KP Records

SECTION 6 SERVICE AVAILABILITY AND RESTORATION REQUIREMENTS

Given that the MBIS will operate under a COOP to include a Disaster Recovery Site (COOP Site), it is anticipated that MBIS Services will have a very high level of continuous availability.

The Service Availability of all MBIS Services must be at a minimum 99.8 percent (99.8%) per month without any allowance beyond 99.8 percent (99.8%) for Scheduled Downtime or switchover from the Primary Site to the COOP Site (or vice versa). Service Availability of 99.8 percent (99.8%) leaves a little less than 90 minutes a month for Service outages at the MBIS level. Contractor may roll Scheduled Downtime between the Primary Site and COOP Site to preclude as many MBIS Service outages as possible. The reasons for the COOP Site include:

- To provide for fast recovery for failed equipment and localized power outages at the Primary Site with 99.8 (99.8%) percent Service Availability as a requirement. This includes provision of any and all Necessary power conditioning and alternative power sourcing to maintain the Service Availability requirement.
- To provide the basis for recovery of services in the event of a catastrophic failure at the Primary Site (fire, explosion, radioactive contaminations, etc.).

SECTION 7 SYSTEM MAINTENANCE REQUIREMENTS

Contractor shall perform Preventive Maintenance and Corrective Maintenance as a part of the monthly Service Fee and at no additional cost to County.

SECTION 7.1 PREVENTIVE MAINTENANCE

Unless agreed to otherwise in advance by County and Contractor, Contractor shall provide all Preventive Maintenance Services during Scheduled Downtime, during late evening hours or early morning hours in order to avoid times when users need to use the System, as agreed to by County.

Contractor will perform a documented Preventive Maintenance procedure for all equipment and software they provide. Contractor shall periodically dispatch maintenance personnel to clean, inspect and adjust the equipment and replace defective or worn parts thereof at the manufacturer's recommended frequency in order to keep the equipment in good operating condition. Contractor shall carry out periodic maintenance tasks on all electronic components they provide to ensure they are operating at maximum capability. Such maintenance shall be scheduled to be performed, at a minimum, once a month during hours agreed to by County.

SECTION 7.2 CORRECTIVE MAINTENANCE

Contractor shall provide corrective maintenance for any Deficiency in Contractor provided equipment or software that, when used as delivered, fails to perform in accordance with the Specifications specified in the Agreement, including System Requirements. The period for the provision of corrective Maintenance coverage for all hardware and software shall be defined as 24/7.

Contractor shall maintain an electronic report log that indicates the problem report number, problem description, the time that the problem call was received, the priority assigned, all actions taken and the time that the problem was corrected. The problem report log shall be maintained in a database that is remotely accessible by County personnel.

Contractor shall offer one central point of contact for support of hardware and software. Contractor support personnel shall address all problems reported by County's Help Desk staff. Contractor's support personnel shall acknowledge problems reported via telephone or by e-mail within one (1) hour and respond according to the protocols listed below.

SECTION 7.3 PROTOCOLS

County shall assign the Priority Level to each Deficiency reported by County to Contractor's Customer Support. Contractor shall assign Priority Levels to Deficiencies discovered by its own problem monitoring system. Following report of a Deficiency from County, Contractor shall respond back to County within the prescribed "Response Timeframe" specified below and resolve each such Deficiency within the specified "Resolution Time". Resolution Time for correction of Deficiencies shall start tolling when County first notifies Contractor of a Deficiency by telephone or otherwise as specified herein, including Contractor's Customer Support, and shall end when County determines that the Deficiency has been resolved.

Problems that require an immediate response (Priority Level 1) are System or component failures that prevent subjects from being enrolled, images from being searched or responses from being delivered. This includes all equipment supplied by Contractor associated with the System, including Remote Site printers, scanners and other required peripherals that would prevent users from accomplishing their work.

Contractor may attempt to correct the problem by phone or remote access. If Contractor is unable to correct the problem in this manner, Contractor must begin on-site repair within four (4) hours of the time Contractor was initially notified, depending on the availability of the site where the equipment resides. All situations that prevent the initiation of on-site repair within such four (4) hours will be documented in Contractor's electronic report log and reported to County's Help Desk.

Contractor must ensure that the equipment will be repaired within eight (8) consecutive hours. If a device is out of service for eight (8) consecutive hours from the time Contractor was notified, Contractor shall, by the end of the eighth hour, replace the defective equipment with an operable device until the defective item has been fully repaired. The eight (8) hour clock begins from the time of personal notification to Contractor.

All other Major Deficiencies (Priority Level 2) will be corrected within two (2) Business Days from the time the problem was reported.

Contractor shall inform County within 1 hour of any service interruptions and then notify the County within eight (8) hours of any hardware or software problems that Contractor has identified and resolved.

ATTACHMENT A.4 – SYSTEM CONFIGURATION

CONTAINS INFORMATION PROPRIETARY AND/OR CONFIDENTIAL TO CONTRACTOR

ATTACHMENT A.5 – EXISTING SYSTEM REPORT

INCORPORATED BY REFERENCE

EXHIBIT A
STATEMENT OF WORK
FOR
MBIS SOLUTION

ATTACHMENT A.1
SYSTEM REQUIREMENTS
FOR
MBIS SOLUTION

ATTACHMENT A.1

SYSTEM REQUIREMENTS

This Attachment A.1 contains MBIS System Requirements for the MBIS Solution to be provided by Contractor under the Agreement.

1. FUNCTIONAL REQUIREMENTS - TENPRINT

High-level functional identification service requirements will be the focus of the tenprint operations group. We will look to utilize the contemporary approach to requirements setting that has been successfully been used as a best practice of peer agencies in the most recent procurement efforts. The goal of this approach is for the Contractor to identify, at a high-level, what functions we perform and require, and let the Contractors bring their solution for accomplishing those functions to bear in a proposal.

Each of the elements of ID services are defined and the associated requirements stated in this section. Identification Services use fingerprint data collected from subjects to launch searches of prior enrollments to determine whether the subject has been previously encountered and enrolled in the MBIS Solution.

1.1 OVERALL SERVICE REQUIREMENTS CATEGORIES

- Tenprint Rapid ID (Identification-Only (IDN)) Services
- Tenprint Identification Services
- Input
- Processing
- Outputs
- NIST Image Retrieval

1.2 TENPRINT RAPID ID SERVICE REQUIREMENTS

This workflow is for the rapid searching (Identification-Only (IDN)) of MBIS and, in turn, CalDOJ or the FBI. If no identity is determined at MBIS, the transaction is submitted to both CalDOJ and the FBI, with or without local ID, as a TPIS (for a 2-minute FBI turnaround) against the entire NGI repository. Tenprint rapid ID service specifications are organized under one of the three categories below:

- **Input** – The tenprint data will be transmitted as EBTS files. These will be rapid turnaround transactions set to the highest priority by the MBIS, if not already set as such by the submitting device. At the MBIS all records will be parsed for compliance with the EBTS. Transactions that fail the parsing test will be logged and returned to the submitting device with an ERRT response.
- **Processing** – The MBIS will process tenprint rapid ID transactions received at the highest system priority level. The fingerprint images will be feature extracted and searched “without add.” Matcher results will be made available via EBTS responses. Based on the submittal data, the transaction is also forwarded to CalDOJ and the FBI for further searching against their Identification system.
- **Output** – The MBIS will prepare responses to all tenprint rapid ID transactions received. If the transaction failed to pass the various checks above, then it will have already produced an error message, pursuant to the EBTS.

Table 1: Rapid Identification TOTs Supported

TOT	TRANSACTION NAME
TPIS	Tenprint Fingerprint Image Search

Table 2: Tenprint Rapid ID Service Requirements

ID	REQUIREMENT
INPUT	
RID Input 1	The MBIS SHALL be able to ingest TPIS transactions and parse them for compliance with the EBTS to include checking for duplicate TCNs.
RID Input 2	The MBIS SHALL be able to forward the acceptable transactions to the local criminal records system to solicit any biometric-based candidates.
RID Input 3	The MBIS SHALL be able to ingest EBTS responses from any appropriate standards-based repository.
RID Input 4	The MBIS SHALL process the acceptable TPIS transactions at the priority set to 1 (the highest priority value).
RID Input 5	The MBIS SHALL record in a log the results of each TPIS transaction ingested.
RID Input 6	The MBIS SHALL store in a temporary file a copy of each TPIS forwarded for processing.
RID Input 7	The MBIS SHALL record a copy of each ingested TPIS transaction in a separate searchable file and in the ANSI/NIST Archive in the fully EBTS compliant form in which it was received.
PROCESSING	
RID Proc 1	The MBIS SHALL “feature extract” the fingerprint images and create an appropriate internal search of the matchers (TP-TP).
RID Proc 2	The MBIS SHALL automatically prepare and return an ERRT response containing the original TCN and Incident ID for all transactions that were not processable.
RID Proc 3	The MBIS SHALL automatically execute all TP-TP searches using the features extracted.
RID Proc 4	If the matcher score for a biometric-based candidate or a technical candidate is above a settable threshold, the MBIS SHALL automatically add that subject to the candidate list (presented in configurable order), with any biometric-based strong candidate in the number one position.
RID Proc 5	The MBIS SHALL forward transactions to CalDOJ and the FBI’s NGI if a search was requested and regardless of a match at MBIS. All TCNs are then forwarded to CalDOJ and the FBI’s NGI.
RID Proc 6	The MBIS SHALL ingest the FBI responses (SRT, TPRR, and ERRT).
RID Proc 7	The MBIS SHALL automatically log all TPIS search transaction results (local, CalDOJ, and FBI) to include the Type 1 fields, time received, time logged at end of processing, and the results.

ID	REQUIREMENT
OUTPUT	
RID Output 1	If there are any candidates available, then the MBIS SHALL automatically return a response TOT with the configurable number of highest scoring candidates.
RID Output 2	If there are no candidates available, then the MBIS SHALL automatically return a response TOT with that information.
RID Output 3	The MBIS SHALL automatically forward CalDOJ and FBI responses (SRT, TPRR, and ERRT) to the originating device.
RID Output 4	The MBIS SHALL automatically add response transactions (SRT, TPRR, and ERRT) to the ANSI/NIST Archive.

1.3 TENPRINT IDENTIFICATION SERVICES REQUIREMENTS

Tenprint identification service specifications are organized under one of the three categories below:

- **Input** – Tenprint identification transaction data is transmitted as EBTS files or paper forms (e.g., inked cards) to MBIS for preprocessing. Inked forms will be converted to appropriate EBTS transactions, and they will be handled by the requirements below. The input TOTs associated with tenprint identification services are listed in the table below.
- **Processing** – The MBIS processes identification transactions received from the various livescan devices and external systems. The various biometric modality data (fingerprint and palmprints) will be sent to the appropriate back-end matchers.
- **Output** – The MBIS prepares responses to all transactions received (i.e., from Live-Scans, other systems, etc.). If the transaction failed to pass the various checks above then it will have already produced an error message in the Input stage, above.

Table 3: Identification TOTs Supported

TOT	TRANSACTION NAME
CRM	Criminal
CUS	Custody
REG	Registrant
SUP	Supplemental
APP	Applicant
IDN	Identification
DEU	Coroners

Table 4: Tenprint Identification Services Requirements

ID	REQUIREMENT
INPUT	
TID Input 1	For paper forms (cards) submitted, the MBIS SHALL provide the user with the capability to scan the image portions of inked fingerprint and palmprint cards at 1,000 pixels per inch (ppi) using FBI-certified Appendix F scanner systems and assign a unique TCN, pursuant to the EBTS.
TID Input 2	For paper forms (cards) submitted, the MBIS SHALL support the scanning of the entire front and back of the cards at 250 or 300 ppi as Type 20 records and link the image(s) with the friction ridge image entry per ID Input 1.
TID Input 3	For paper forms (cards) submitted, the MBIS SHALL provide the user with the capability of entering card field text, pursuant to the EBTS, and linking the text fields (Types 1 and 2) with the appropriate scanned images per ID Input 1 and 2.
TID Input 4	For paper forms (cards) submitted, after scanning and text entry are complete [ID Input 1 through ID Input 3], the MBIS SHALL automatically create a complete EBTS Transaction with the Record Types 1, 2, 14, 15, and 20, as appropriate, using an appropriate TOT from the Identification TOT table.
TID Input 5	The MBIS SHALL be able to ingest EBTS transactions as listed in the Identification TOT table above, and parse them for compliance with the EBTS to include checking for duplicate TCNs.
TID Input 6	The MBIS SHALL be able to quality check (i.e., fingerprint quality via NFIQ, sequence, and presence of spurious fingers) the friction ridge images of ingested and created EBTS transactions against adjustable quality thresholds (NFIQ threshold and non-recoverable sequence errors).
TID Input 7	The MBIS SHALL forward the transactions that fail the automated quality checks [TID Input 6] to appropriate examiner work queues for examiner-assisted QC.
TID Input 8	The MBIS SHALL permit examiners to selectively pick a transaction from the QC queue and present the selected transaction's images within 4 seconds of the selection.
TID Input 9	The MBIS SHALL provide support to examiners in performing QC activities (adjust sequence, correct or establish the pattern, center images, to include rejecting a transaction) and responding to the livescan station when finished.
TID Input 10	The MBIS SHALL log the NFIQ score for each rolled finger in a retrievable format to include finger number, and all Type 1 field data, independent of the transaction passing or failing the automated QC [TID Input 7].
TID Input 11	The MBIS SHALL be able to respond to the noncompliant or unacceptable image quality transactions via an EBTS ERRT.
TID Input 12	The MBIS SHALL be able to forward the acceptable transactions to the local criminal records repository to solicit any biometric-based candidates via an EBTS transaction.
TID Input 13	The MBIS SHALL be able to ingest EBTS responses from any appropriate standards-based repository..

ID	REQUIREMENT
TID Input 14	The MBIS SHALL update the original ingested transaction with information from the criminal records repository response.
TID Input 15	The MBIS SHALL update the log entry for each transaction with the results of each EBTS ingested.
TID Input 16	The MBIS SHALL store in a temporary file a copy of each EBTS forwarded for processing.
TID Input 17	The MBIS SHALL be able to ingest EBTS transactions received from the various livescan devices and external systems (cross-jurisdictional searches).
TID Input 18	The MBIS SHALL parse ingested EBTS transactions from external systems checking for compliance with the EBTS to include checking for duplicate TCNs.
TID Input 19	The MBIS SHALL be able to respond to the noncompliant transactions via an EBTS EERR.
TID Input 20	The MBIS SHALL record a copy of each ingested transaction in the ANSI/NIST Archive.
PROCESSING	
TID Proc 1	<p>The MBIS SHALL provide full configurability, by a system administrator, minimally for the following system dimensions:</p> <ul style="list-style-type: none"> • Number of candidates presented on a list • Ordering of the candidates on a list (score v. random) • Hide/Unhide scores, demographics and mugshots • Number of verification steps utilized • Matching threshold scores <p>at the user, group, agency, or other security designation level.</p>
TID Proc 2	The MBIS SHALL “feature extract” all friction ridge images and create appropriate internal TP-TP searches of the matchers, and cascade TP-LT, and KP-LT internal searches based on the record types (4, 14, and 15) in the transaction for all transactions.
TID Proc 3	The MBIS SHALL automatically execute all searches created in TID Input 1.
TID Proc 4	If the TP-TP matcher score for a biometric-based searched candidate is above a configurable threshold (#1), then the MBIS SHALL automatically declare a match.
TID Proc 5	If the TP-TP matcher score for a technical search candidate is above a settable threshold (#2), then the MBIS SHALL automatically declare a match.
TID Proc 6	If the matcher score for all candidates is below a settable threshold (#3), then the MBIS SHALL automatically declare a no-match.

ID	REQUIREMENT
TID Proc 7	If there is no automatic decision (match or no-match) and there are candidates with scores between Thresholds 2 and 3, then the MBIS SHALL create and move a verification package (original images and candidate images and information) to the appropriate examiner work queues for examiner-assisted verification for a configurable number of candidates, to include any candidate in configurable order.
TID Proc 8	The MBIS SHALL permit examiners to selectively pick a transaction from the Verification queue and present the selected transaction's images for at least the search prints and the first candidates within 4 seconds of the selection.
TID Proc 9	The MBIS SHALL provide support for examiners to verify candidates for searches selected from the queue and to selectively manipulate the original image and the candidate image separately or in synchrony (i.e., zoom, magnify, and rotate; and adjust contrast, brightness, and sharpness), mark points of similarity, draw along ridges in color as well as use hyperlinked fields in the candidate entries to go to the Master ID cross-reference file or to a specific archived transaction.
TID Proc 10	The MBIS SHALL support a configurable number of (at least two) additional blind verification steps are needed to retain the steps we currently have for 2 nd verification and 3 rd verification. 3 rd verification is technical review if there is disagreement between 1 st and 2 nd verification. We still need to articulate some kind of electronic verification in MBIS.
TID Proc 11	The MBIS SHALL permit the examiners to print any search or candidate fingerprint set with Type 1 and Type 2 data.
TID Proc 12	In the case of an automatic or manual no-hit decision where the retention code, field 1.06, is set to Y, the MBIS SHALL establish a new MAIN.
TID Proc 13	The MBIS SHALL be able to ingest EBTS response transactions (SRE and ERRT) from the CalDOJ, and any other external systems where a search was requested in Field 2.098 NDR and store an original copy of the response in the ANSI/NIST Archive.
TID Proc 14	The MBIS SHALL use the response information from the external systems to update the master identity files and the transaction log.
TID Proc 15	The MBIS SHALL establish and maintain a master identity for each subject enrolled – to include links to all successfully processed transactions' TCNs, and associated MAINs.
TID Proc 16	The MBIS SHALL automatically log all search transaction results to include the original Type 1 fields, time received, time at end of processing, and the results.
TID Proc 17	The MBIS SHALL support the enrollment of tenprints and palm prints in the search database as individual records-without limit, as well as supporting a composite. Contractor should explain their record store/search processing best practice or philosophies (for example, keep all/search all or create composite with last 3 most recent events).

ID	REQUIREMENT
TID Proc 18	The MBIS SHALL support and facilitate subject updates, especially for large quantity updates linked by a numerical identifier.
TID Proc 19	The MBIS SHALL support and facilitate the ability, based on user authorization, to change the processing priority for transactions, including the stopping of a transaction.
OUTPUT	
TID Output 1	The MBIS SHALL automatically prepare and return an SRE response containing the original TCN and Incident ID for all transactions where the subject was successfully searched – showing the results (for hit and no-hit).
TID Output 2	The MBIS SHALL automatically forward any external system SREs and ERRTs to the submitting agency or department.
TID Output 3	The MBIS SHALL automatically prepare and return an ERRT response containing the original TCN and Incident ID for all transactions where the transaction was not processable.
TID Output 4	The MBIS SHALL automatically add response transactions (SRE and ERRT) to the ANSI/NIST Archive, as well as in the transaction log.
TID Output 5	The MBIS SHALL automatically send an SRE to the appropriate criminal records repository system.
TID Output 6	The MBIS SHALL support the ability to create and update a configurable number of footer messages (message stamps) that are then included with identified transaction outputs.
TID Output 7	<p>The MBIS SHALL support a post-processing queue reporting/logging capability</p> <ul style="list-style-type: none"> • Transaction logging • Response tracking • Ability to recall the booking and response, and e-mail it. • Use dual screens in post-processing to see multiple bookings
TID Output 8	<p>The MBIS SHALL support the searching of the sealed records queue by a configurable number of key record numbers such as;</p> <ul style="list-style-type: none"> • Booking number • Main number • SID, FBI or TCN.

1.4 NIST IMAGE RETRIEVAL REQUIREMENTS

This section outlines the requirements for the various inputs, processing, and outputs for NIST image retrieval.

Table 5: NIST Image Retrieval Requirements

ID	REQUIREMENT
INPUT	
Image Retr In 1	The MBIS SHALL be able to ingest EBTS transactions and parse them for compliance with the EBTS to include checking for duplicate TCNs.
Image Retr In 2	The MBIS SHALL be able to respond to the noncompliant transactions via an EBTS ERRT to the criminal records repository.
Image Retr In 3	The MBIS SHALL provide the ability for the user to create transactions using pull-down menus or manually entering the Type 2 fields.
Image Retr In 4	The MBIS SHALL forward the acceptable transactions for processing.
Image Retr In 5	The MBIS SHALL record in a log the results of each EBTS ingested.
Image Retr In 6	The MBIS SHALL store in a temporary file a copy of each EBTS forwarded for processing.
Image Retr In 7	The MBIS SHALL be able to ingest EBTS transactions received from the various livescan or input devices and external systems.
Image Retr In 8	The MBIS SHALL record a copy of each ingested transaction in the ANSI/NIST Archive in the fully EBTS compliant form in which it was received.
PROCESSING	
Image Retr Proc 1	The MBIS SHALL process the EBTS transactions [Image Update In 7] and determine whether the requested image is available.
Image Retr Proc 2	If the image is not available it SHALL forward image retrieval transactions to the CalDOJ system.
Image Retr Proc 3	The MBIS SHALL be able to ingest responses from the CalDOJ.
Image Retr Proc 4	The MBIS SHALL use the response information from the CalDOJ and FBI NGI processing to update the transaction log.
OUTPUT	
Image Retr Out 1	The MBIS SHALL automatically forward any internal or external system response transactions to the submitting criminal records repository or user/ORI.
Image Retr Out 2	The MBIS SHALL automatically add response transactions to the ANSI/NIST Archive.

2. FUNCTIONAL REQUIREMENTS – LATENT

High-level functional latent service requirements will be the focus of the latent operations group. We will look to utilize the contemporary approach to requirements setting that has been successfully used as a best practice of peer agencies in the most recent procurement efforts. The goal of this approach is for the Contractor to identify, at a high-level, what functions we perform and require, and let the Contractors bring their solution for accomplishing those functions to bear in a proposal.

Each element of latent services are defined and the associated requirements stated in this section. Latent services use partial fingerprint data collected from subjects to launch searches of prior enrollments to determine whether the subject has been previously encountered and enrolled in the MBIS Solution.

2.1 OVERALL SERVICE REQUIREMENTS CATEGORIES

- Reverse Latent Services:
 - Input
 - Processing
 - Outputs
- Forward Latent Services:
 - Input
 - Processing
 - Outputs
- Latent Case Management Services

This section addresses requirements relative to latent processing. Additionally, subsections here present how peer agencies address similar functions. Final subsections here allow for the approval of requirements to be promoted to the MBIS Solution RFP.

Table 6: Latent ID TOT Supported

TOT	TRANSACTION NAME
ULM	Unsolved Latent Match Response

2.2 REVERSE LATENT SERVICE REQUIREMENTS

All identification transactions containing fingerprint or palmprint records (and marked as “add to MBIS”) will be automatically reverse-searched against the unsolved latent. The reverse search occurs in the course of input phase of tenprint identification services. Reverse latent identification service specifications are organized under one of the three categories below:

- **Input** – The input TOTs are listed above. They can originate within MBIS or the FBI’s NGI system. If they start within MBIS, they are sent to the appropriate owner of the unsolved latent print, and sent to the generic ULM queue accessible to all users. If they originate at the FBI, they are sent to MBIS and in turn distributed to the owner where the latent was enrolled in the unsolved latent file, and sent to the generic ULM queue accessible to all users.
- **Processing** – If an unsolicited latent match response is received from the FBI, it is logged, added to the ANSI/NIST Archive, and forwarded to the appropriate owner. It is anticipated that only one candidate will be returned per ULM transaction.
- **Output** – The MBIS will permit the examiner to document the results of the examination of the ULM and associated friction ridge material.

Table 7: Reverse Latent Service Requirements

ID	REQUIREMENT
INPUT	
RL Input 1	The MBIS SHALL be able to ingest EBTS transactions as responses from searches made in response to tenprint identification service input.
RL Input 2	The MBIS SHALL be able to ingest EBTS transactions from the state ULM .
RL Input 3	The MBIS SHALL record in a log the results of each EBTS ingested.
RL Input 4	The MBIS SHALL store in a temporary file a copy of each EBTS forwarded to the MBIS.
RL Input 5	The MBIS SHALL be able to ingest EBTS transactions received from the various latent stations.
RL Input 6	The MBIS SHALL record a copy of each ingested transaction in the ANSI/NIST Archive in the EBTS compliant form in which it was received.
RL Input 7	The MBIS SHALL support an interface to the CAL DOJ Latent Gateway in order to facilitate the running of a latent through MBIS and CalDOJ without running the latent two separate times.

ID	REQUIREMENT
PROCESSING	
RL Proc 1	<p>The MBIS SHALL provide full configurability, by a system administrator, minimally for the following system dimensions:</p> <ul style="list-style-type: none"> • Number of candidates presented on a list • Ordering of the candidates on a list (score v. random) • Hide/Unhide scores • Masking/unmasking mug shots. • Number of verification steps utilized • Matching threshold scores <p>at the user, group, agency, or other security designation level.</p>
RL Proc 2	The MBIS SHALL process reverse latent transactions at accuracy rate and performance level established in accuracy rate table in section 6.3.
RL Proc 3	The MBIS SHALL add all transactions that are received from the FBI to the ANSI/NIST Archive.
RL Proc 4	The MBIS SHALL forward all transactions that are received from the FBI to the appropriate latent station.
RL Proc 5	The MBIS SHALL create an LCMS entry in the appropriate verification work queue for each transaction that is received.
RL Proc 6	The MBIS SHALL support examiners in selectively picking a transaction from the Verification queue.
RL Proc 7	The MBIS SHALL support the examiners in the verification of candidates for searches selected from the queue by providing the associated friction ridge images (reverse search print and original latent image).
RL Proc 8	The MBIS SHALL support the examiners in the verification of candidates for searches selected from the queue and to selectively manipulate the original image and the candidate image separately or in synchrony (i.e., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, mirror (horizontal or vertical), sharpen/unsharpen, mark points of similarity, draw along ridges in color, apply false color encoding based on image density, conduct ridge counting as necessary, trace feature will be required and generate histograms).
RL Proc 9	The MBIS SHALL permit the examiners to print (1) any search latent at 1:1 or 5:1 size for latent images with case number and image number as well as time and date printed or (2) any candidate fingerprint/palmprint set with Type 1 and Type 2 data for tenprint and palmprint cards (ten print or palm print card in the standard FBI-14 format).
RL Proc 10	The MBIS SHALL support the forensic examiner selectively declaring a match, returning the transaction to the work queue, or forwarding the transaction to another examiner for confirmation or advice.
RL Proc 11	The MBIS SHALL automatically log all reverse friction ridge search transactions and the steps taken, the examiners involved, and the search results in the LCMS.

ID	REQUIREMENT
RL Proc 12	The MBIS SHALL support the preparation of court presentations when a match is found in any reverse latent search.
RL Proc 13	The MBIS SHALL automatically log all reverse latent search transactions and the examiners' results in the system log and LCMS.
RL Proc 14	The MBIS SHOULD be able to support prevention of the unnecessary and redundant returns of same, non-mated candidate(s) appearing for each subsequent reverse search for each single impression in ULM, by the setting of the threshold for a reverse search based on the original highest score for that latent, when it was run against the entire database, or by other means.
RL Proc 15	The MBIS SHOULD be able to support auto correction of the orientation of the latent to the exemplar when displayed side by side for comparison.
RL Proc 16	<p>The MBIS SHOULD be able to support:</p> <ul style="list-style-type: none"> • No required ridge counting on entry to new MBIS system. • No required setting of core/axis on entry to new MBIS system. • Processing of merged candidate lists • Multiple minutia sets. • Scaling a print based on ridge density.
RL Proc 17	The MBIS SHOULD be able to support a minimum latent search response time of less than 1 minute.
RL Proc 18	The MBIS SHOULD be able to support the capability of pulling a latent from unsolved latent database and re-launch a latent search.
RL Proc 19	The MBIS SHOULD be able to support the searching of the entire friction ridge area of the hand, including terminal, mid and basal phalanges (County uses OC's Proximal, medial and distal) with the capture of the complete palm image.
RL Proc 20	The MBIS SHOULD be able to support fully configurable (by agency administrators) field sizes to account for different ways Los Angeles County agencies do business. As an example, Sheriff's case numbers are 18 long but the current field is much shorter.
RL Proc 21	The MBIS SHOULD be able to support the routing of messages by ORI numbers and "submitting" ORI numbers which will allow for cases to be submitted from "satellite" sites by an examiner from a different agency or unit. This would allow hit messages to be sent to the agency that submitted the case, instead of the agency where the terminal is and to allow statistical information to be gathered for agencies that do not have a LAFIS terminal.
RL Proc 22	The MBIS SHOULD be able to support fully configurable (by agency administrators) field sizes in order to enter sufficient information to identify case, allowing the examiner to insert enough information to keep track of the case, without having to go to the file to look at it.
RL Proc 23	The MBIS SHOULD be able to support robust terminals capable of allowing programs, such as "PhotoShop," to be installed without adversely affecting the operation of the machine.

ID	REQUIREMENT
RL Proc 24	The MBIS SHOULD be able to support access to the Cal-DOJ Automated Archive System by all terminals.
RL Proc 25	The MBIS SHOULD be able to support a mechanism to search dissimilar MBIS systems without any additional capture of latent images and bring back the results to the Queue in the LACRIS MBIS. The results (side by sides) will be able to be viewed with the same tools available in viewing prints from the LACRIS MBIS.
RL Proc 26	The MBIS SHOULD be able to support the auto-population of any field repeated on previous or subsequent screens, if the information for these fields is the same.
RL Proc 27	The MBIS SHOULD be able to support the full use of the scanning surface, to allow for the scanning of multiple cards of different sizes simultaneously.
RL Proc 28	The MBIS SHOULD be able to support the merging of individual latents from separate cases into a single candidate list.
RL Proc 29	The MBIS SHOULD be able to support the searching of, at least, the last six arrest records, if available, (flats, rolls and palms).
RL Proc 30	The MBIS SHOULD be able to support the maintaining all arrest fingerprint records (Palm and Finger) in the appropriate MBIS database.
RL Proc 31	The MBIS SHOULD be able to support the searching of all archive records in the MBIS data base. (for sealing and record correction)
RL Proc 32	The MBIS SHOULD be able to support equal or better quality of printed exemplars as the ones received now from our archive system.
RL Proc 33	<p>The MBIS SHOULD be able to support the printing of exemplars where the notation is automatically added at the bottom to indicate what database it came from and the name of the operator who printed it out and the date it was printed out. Examples include but are not limited to:</p> <ul style="list-style-type: none"> • <i>THE IMAGES AND/OR DATA CONTAINED HEREIN WERE OBTAINED FROM THE LOS ANGELES COUNTY REGIONAL</i> • <i>IDENTIFICATION SYSTEM ARCHIVE AND ARE RESTRICTED FOR OFFICIAL LAW ENFORCEMENT USE ONLY.</i> • <i>****NOTE****THESE IMAGES AND DATA ARE PART OF THE ORIGINAL NIST FILE IN THE LIVESCAN</i> • <i>IDENTIFICATION REQUEST RECEIVED BY LACRIS. ****NOTE****</i>
RL Proc 34	The MBIS SHALL support and accept photoshop files seamlessly, and automatically resize the image(s) as necessary.
RL Proc 35	The MBIS SHALL support the option to search other standards-based MBIS systems regardless of the provider.
RL Proc 36	The MBIS SHALL support capturing and transmitting latent prints at crime scene directly to MBIS terminal via a handheld device.
RL Proc 37	The MBIS SHALL support the option of changing the size and shape of the capture box used to clip prints from scanned latent print cards.

ID	REQUIREMENT
RL Proc 38	The MBIS SHALL support Printouts that have palm latent print image next to candidate image with case information below needs to include the CII# .
RL Proc 39	The MBIS SHALL support logs showing updates to system, maintenance, and scheduled down time for each MBIS terminal.
RL Proc 40	The MBIS SHALL support the searching palm latents 360 degrees.
RL Proc 41	The MBIS SHALL support the searching latents using third level detail.
RL Proc 42	The MBIS SHALL support the need to be able to run a latent inquiry (LFFS) without creating case and without registering in ULM.
RL Proc 43	The MBIS SHALL support Latent/TP comparison software for court exhibits.
OUTPUT	
RL Output 1	The MBIS SHALL automatically prepare a LCMS report for all reverse latent searches.
RL Output 2	The MBIS SHALL support the examiner in selecting to (1) mark the case as closed or (2) simply save and close the LCMS file.
RL Output 3	The MBIS SHALL maintain a searchable log of all reverse latent searches submitted to the MBIS by external systems and to the latent stations from the MBIS.
RL Output 4	The MBIS SHALL support reporting functionality at any latent workstation, including: <ul style="list-style-type: none"> • Reporting on the originator of a print search. • Upon request, print the latent on left and the rolled image on right on the same page.
RL Output 5	The MBIS SHALL support the ability to print the latent search image, transaction number, and the list of all subjects by criminal identifier numbers that appear on the candidate list, all on one page.

2.3 FORWARD LATENT SERVICE REQUIREMENTS

This section describes the requirements involving any FIS transaction types used.

Table 8: Mobile ID TOT Supported

TOT	TRANSACTION NAME
LFFS	Latent Fingerprint Features Search
LFIS	Latent Fingerprint Image Search

Forward latent searches use latent fingerprint and palmprint samples collected at crime scenes and disaster victim fingerprints, as well as fingerprints from deceased subjects collected by morgues, to determine whether the subject has been previously encountered and enrolled in the MBIS system. External agencies, using Universal Latent Workstations (ULW), can also submit forward latent searches.

Forward latent identification service specifications are organized under one of the three categories below:

- **Input** – The input TOTs are listed above. Collection will typically start with:
 - A crime scene technician or investigator collecting images or other friction ridge samples at a crime scene.
 - A forensic scientist examining an item of evidence (e.g., an unfired round in a gun) and imaging a latent fingerprint or palmprint.
 - A medical examiner collecting friction ridge samples from a deceased person.
 - A disaster response team providing DVI services where fingerprints are typically harvested from whatever portions of a hand that can be found and used – this is different from an Identification Service search of good quality tenprints collected at the morgue post mortem using the DEK or DEU TOT for a TP-TP Identification search.

In each case, along with an image, other case-related information will be supplied, such as date collected, unique identification number of the image or sample, the point of contact where results should be reported, collection location, crime type or morgue case type, etc. The images and information will be entered through a workstation and transmitted to the MBIS via a LCMS. The LCMS will provide tracking of the processing of the latent through all searches to include maintaining a log of searches, image processing, candidates, etc. The LCMS will provide the ability for examiners to query status and other attributes of latent submittals and cases as well as to return to open cases as often and whenever they see fit. Transactions entered through ULWs from external agencies will be entered through the LCMS for tracking and reporting purposes.

- **Processing** – The examiner will forward the latent transactions with the impression and tracking information to the LCMS for forensic processing as an LFFS transaction type.
 - The LCMS will queue the latent transaction for a latent examiner to select and process, or if the transaction originated from a ULW or cross-jurisdictional partner, it will be auto-launched without any examiner action – as a lights-out remote search. Since the MBIS will not know whether the remote submitter made an identification, these submittals will not be automatically forwarded to the FBI – but rather the agency will have to resubmit them for forwarding. Cross-jurisdictional partners will not use MBIS to forward searches to the FBI, as they have their own paths to that service.
 - The examiner will perform pre-search steps (rotate, crop, mark and edit minutiae, etc.) before submitting a search. This will be performed using latent editing software integrated into the MBIS software, to include Photoshop.
 - The examiner will be able to limit the search by crime type, finger or palm position, geographical region where the crime was committed, and other traditional parameters or elect to use no search limitations. The MBIS will search the record against known records as well as against unsolved latent records. The known record files for latent searches to run against, sometimes referred to as the “latent cognizant files,” will contain up to three instances of known fingerprints and one of palmprints enrolled in the system rather than just a single set of best images.
- **Output** – The MBIS will prepare responses to all forward latent transactions received. The examiners will be given the opportunity to forward unsolved latents to the FBI, to add them to the MBIS unsolved latent file, to edit and resubmit them, or to save them for future work. If there is a match, then the identity of the subject is returned to the submitting agency. If there is no match and the latent sample is selectively added to the unsolved latent file, it will be reverse searched against all subsequent transactions that include fingerprint and palmprint data.

Table 9: Forward Latent Service Requirements

ID	REQUIREMENT
INPUT	
FL Input 1	<p>The MBIS SHALL support the examiners in creation of a new case in the appropriate LCMS to include entering data in the case information fields as well as the following image fields per image:</p> <p>Latent collection location.</p> <p>“Method of processing” using a pull-down menu.</p>
FL Input 2	<p>The MBIS SHALL support the ingesting of digital images with latent fingerprints or palmprints captured at various scales as Type 13 images into a specific case using a pull-down menu of cases associated with the examiner’s agency (via scanned image, CD, flash drive, etc.).</p>
FL Input 3	<p>The MBIS SHALL support the scanning of latent friction ridge material into Type 13 images at 1:1 scale, 1,000 ppi, 8-bit gray scale, along with a ruler for calculating/verifying scale and resolution into a specific case using a pull-down menu of cases associated with the examiner’s agency.</p>
FL Input 4	<p>The MBIS SHALL support the imaging with a high resolution digital camera of latent friction ridge material as Type 13 images at 1:1 scale, 1,000 ppi, 8-bit gray scale, along with a ruler for calculating/verifying scale and resolution into a specific case using a pull-down menu of cases associated with the examiner’s agency.</p>
FL Input 5	<p>The MBIS SHALL support the ingesting of latent case textual information linked to a latent image as Type 2 fields from a text file or the keyboard into a specific case using a pull-down menu of cases associated with the examiner’s agency.</p>
FL Input 6	<p>The MBIS SHALL support the scanning of inked fingerprints into Type 13 images from deceased persons at 1,000 ppi, 8-bit gray scale into a specific case using a pull-down menu of cases associated.</p>
FL Input 7	<p>The MBIS SHALL support the ingesting of crime scene and object reference images selectively as Type 20 and Type 21 images for use in the LCMS into a specific case using a pull-down menu of cases associated.</p>
FL Input 8	<p>The MBIS SHALL ingest LFFSs submitted from ULWs at outside agencies, after logging them into the LCMS, set them for auto run.</p>
FL Input 9	<p>The MBIS SHALL support the examiner in selectively creating an LFFS package for each latent image in a case, with the appropriate Type 1, Type 2, Type 13, and Type 20 records, and store it in the LCMS as an LFFS.</p>
FL Input 10	<p>The MBIS SHALL update the LCMS logs with the results of each step in the forensic services input process.</p>

ID	REQUIREMENT
PROCESSING	
FL Proc 1	<p>The MBIS SHALL provide full configurability, by a system administrator, minimally for the following system dimensions:</p> <ul style="list-style-type: none"> • Number of candidates presented on a list • Ordering of the candidates on a list (score v. random) • Hide/Unhide scores • Masking/unmasking mug shots. • Number of verification steps utilized • Matching threshold scores <p>at the user, group, agency, or other security designation level..</p>
FL Proc 2	The MBIS SHALL process forward latent transactions at accuracy rate and performance level established in accuracy rate table in section 6.3.
FL Proc 3	The MBIS SHALL automatically queue the latent transaction within the LCMS.
FL Proc 4	The MBIS SHALL permit a forensic examiner to select a transaction for preprocessing from the work queue.
FL Proc 5	The MBIS SHALL support the preprocessing of Type 13 latent images to include image processing (i.e., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, apply a Fast Fourier Transform (FFT), mirror (horizontal or vertical), sharpen/unsharpen, mark features, apply false color encoding based on image density, generate histograms, and select a region of interest) and save the results to LCMS.
FL Proc 6	The MBIS SHALL selectively export from the LCMS the Type 13 for preprocessing on another system
FL Proc 7	The MBIS SHALL import to the LCMS Type 13 images that were preprocessed on other systems.
FL Proc 8	The MBIS SHALL support Examiner in selectively saving and closing the case or submitting it for extraction.
FL Proc 9	The MBIS SHALL support the auto-extraction of features from LCMS transactions using the Extended Feature Set as defined in the ANSI/NIST ITL-1 2011 Standard and save the results to LCMS.
FL Proc 10	The MBIS SHALL support the manual review and editing of features by an examiner and save the results to LCMS.
FL Proc 11	The MBIS SHALL support the creation/editing of search parameters such as selective geographic location, crime type(s), or a specific subject (e.g., a suspect in the case), pattern type, hand, or finger position, to include configurable candidate list length using pull-down menus.

ID	REQUIREMENT
FL Proc 12	The MBIS SHALL support the submittal of forward latent searches selectively against any combination of known fingerprints, palmprints, and unsolved latents on the MBIS where the known fingerprints include all enrolled exemplars – both rolled and plain impressions.
FL Proc 13	The MBIS SHALL automatically search the submitted forward latent searches.
FL Proc 14	The MBIS SHALL build candidate lists of possible matches to forward searches and queue them for forensic examiners to select for verification; candidate Type 2 information shall include sex, DOB, and complete pattern type list.
FL Proc 15	If the latent case was a remote, lights-out search, the MBIS SHALL automatically forward the candidate list to the submitting examiner with the images of the top candidates (a selectable number up to 10).
FL Proc 16	The MBIS SHALL support examiners in selectively picking a transaction from the Verification queue.
FL Proc 17	The MBIS SHALL support the examiners in the verification of candidates for searches selected from the queue by providing the associated friction ridge images, features (search print and first candidate), and a list of Type 2 and record processing history.
FL Proc 18	The MBIS SHALL support the examiners in the verification of candidates for searches selected from the queue and allow them to selectively manipulate the original image and the candidate image separately or in synchrony (i.e., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, apply FFT, mirror [horizontal or vertical], sharpen/unsharpen, mark points of similarity, mark minutiae, draw along ridges, apply false color encoding based on image density, generate histograms, turn on and turn off all minutiae, scaling a print based on ridge density, and display matching minutiae).
FL Proc 19	The MBIS SHALL support the forensic examiner in selectively declaring a tentative match, returning the transaction to the queue, forwarding the transaction to another examiner for confirmation or advice, or editing and resubmitting the search to include manually editing the feature set.
FL Proc 20	The MBIS SHALL support a second forensic examiner selectively selecting a confirmation-verification package and using the tools declaring a match, non-match, or elimination; or editing and resubmitting the search to include manually editing the feature set.
FL Proc 21	The MBIS SHALL automatically log all forward friction ridge search transactions and the steps taken, the examiners involved, and the search results in the LCMS.
FL Proc 22	The MBIS SHALL support the preparation of court presentations when a match is found in any forensic friction ridge search.
FL Proc 23	The MBIS SHALL automatically log all forward latent search transactions and the examiners' results in the system log and LCMS.

ID	REQUIREMENT
OUTPUT	
FL Output 1	The MBIS SHALL automatically prepare a LCMS report for all forensic searches that lead to an identification.
FL Output 2	The MBIS SHALL support the examiner in selecting to (1) add new unsolved latents to the unsolved latent file with a link to the appropriate LCMS records, (2) delete the record, or (3) simply save and close the LCMS file, according to user roles and permissions.
FL Output 3	The MBIS SHALL support the selective forwarding of LFFS transactions to the FBI, first using an LPNQ transaction, if appropriate, or to other systems (e.g., cross-jurisdictional partners) using the EFS or ULW to generate a more appropriate Type 9 record.
FL Output 4	The MBIS SHALL support the ingesting of any response to an LPNQ transaction (an LPNR TOT) automatically forwarding it to the appropriate LCMS case.
FL Output 5	The MBIS SHALL support the ingesting of any response to an LFFS transaction (SRL or ERRL TOTs) automatically forwarding it to the appropriate LCMS case.
FL Output 6	The MBIS SHALL maintain a searchable log of all forensic transactions submitted (along with the responses) to the MBIS and to external systems in the system log and LCMS.
FL Output 7	The MBIS SHALL support the selective forwarding of FBI and other external responses (SRL TOTs) to latent transactions to the appropriate Verification queue.
FL Output 8	The MBIS SHALL automatically log all forward latent search transactions and the examiners' results in the system log and LCMS.
FL Output 9	The MBIS SHALL support the printing of the actual date and time on every sheet of paper that comes out of the system.
FL Output 10	The MBIS SHALL support true interoperability and the ability to encode "once" and search anywhere.
FL Output 11	The MBIS SHALL support a configurable number of images per candidate.
FL Output 12	<p>The MBIS SHALL support reporting functionality at any latent workstation, including:</p> <ul style="list-style-type: none"> • Reporting on the originator of a print search. • Upon request, print the latent on left and the rolled image on right on the same page.
FL Output 13	The MBIS SHALL support the ability to print the latent search image, transaction number, and the list of all subjects by criminal identifier numbers that appear on the candidate list, all on one page.

2.4 LATENT CASE MANAGEMENT REQUIREMENTS

The LCMS can be used to ingest and launch searches as described and specified in the forward latent services above. The LCMS will support the latent examiners and system administrators in maintaining the MBIS latent files and the LCMS records to include the maintenance of latent cases, images, and reports at the MBIS and CalDOJ levels. Maintenance of latent transactions submitted to the CalDOJ and the FBI will be via the TOTs below, and they will be generated by the LCMS.

The MBIS will process latent management transactions received. The original NIST transactions will be preserved indefinitely in the ANSI/NIST Archive of transactions.

Table 10: Latent Maintenance TOTs

TOT	TRANSACTION NAME
LSMQ	Latent Search Status and Modification Query
ULAC	Unsolved Latent Add Confirm Request
ULD	Unsolved Latent Delete Request

Latent examiners and supervisors will use the LCMS to manage the latent case files.

Table 11: Latent Case Management Requirements

ID	REQUIREMENT
LCMS 1	<p>The MBIS SHALL support latent examiners and system administrators in the creation of latent cases, independent of actually loading any images, to include entering and saving information in the following data fields:</p> <ul style="list-style-type: none">• Case name.• Case number.• Owning agency.• Date of crime.• Date case opened in LCMS.• Examiner the case is assigned to.• Crime Lab reference number.• 4-digit NCIC Uniform Offense Code• State Crime Code(s) – a pull down menu based on the 4-digit Uniform Crime code entered.• Auto delete flag at statute of limitations date (Y/N).• Up to 10 additional free form fields.
LCMS 2	<p>The MBIS SHALL support latent examiners and system administrators in populating and updating a “method of collection” table used in an LCMS pull-down menu of types of collection/processing to include lifts; digital imagery; Alternate Light Source (ALS); ninhydrin, DFO, or other chemical process; deposition processes); and up to 10 others.</p>
LCMS 3	<p>The MBIS SHALL support latent examiners and system administrators in populating and updating a table of statutes of limitations on state crime codes.</p>

ID	REQUIREMENT
LCMS 4	The MBIS SHALL permit and support latent examiners and system administrators in selective maintenance of the LCMS files, unsolved latent file, and matcher files to include correcting incorrectly entered information, moving images between cases, merging cases, and updating the table of statutes of limitations based on state crime codes.
LCMS 5	The MBIS SHALL automatically track all latents submitted to external agencies for retention.
LCMS 6	The MBIS SHALL automatically track for reporting purposes all latents submitted by external agencies.
LCMS 7	The MBIS SHALL automatically identify situations where searches against different latents from the same case have identical candidates anywhere in the top 100 positions and alert the examiner(s) assigned to the case with a message in their work queue.
LCMS 8	The MBIS SHALL offer latent examiners and system administrators the ability to remove latent images from the MBIS and/or an external unsolved latent file(s).
LCMS 9	If latent examiners and system administrators elect to remove a latent image from any external system's unsolved latent file, the MBIS SHALL automatically generate the appropriate TOT.
LCMS 10	The MBIS SHALL automatically alert the system administrator via a message in an administrative queue when a case reaches the following windows: 90, 60, and 30 days from the expiration of the statute of limitations for any and all cases. Ignored alerts will be escalated to the system administrator.
LCMS 11	The MBIS SHALL support the latent examiners and system administrators in selectively opening and dealing with administrative message in their work queue and in relaunching or closing cases where the statute of limitations expired notice has been sent to them.
LCMS 12	The MBIS SHALL automatically delete unsolved cases from the LCMS when the statute of limitations expires if the Auto-Delete flag was set to "Y" in LCMS when the case was opened or at any later point.
LCMS 13	If the LCMS automatically closes a latent case that has any images in an external system's unsolved latent file, the MBIS SHALL automatically generate the appropriate transaction.
LCMS 14	The MBIS SHALL forward latent management transactions to CalDOJ and the FBI's NGI system.
LCMS 15	The MBIS SHALL be able to ingest external system responses from the FBI (ULAR, ULDR, LSMR, and ERRA TOTs).
LCMS 16	The MBIS SHALL use the response information from the FBI to update the transaction log.
LCMS 17	The MBIS SHALL automatically forward any external system response transactions to the appropriate LCMS.

ID	REQUIREMENT
LCMS 18	The MBIS SHALL automatically log all latent management transactions and activities to include date, time, person performing the activity, activity type, status (successful or problem encountered), and any changes to the MBIS or external system matcher files of unsolved latents.
LCMS 19	The MBIS SHALL record a copy of each ingested transaction in the ANSI/NIST Archive in the EBTS compliant form in which it was received.
LCMS 20	<p>The current Case Management System is developed in three phases</p> <ol style="list-style-type: none"> 1. Case 2. Card 3. Latent <p>The Contractor SHOULD be able to explain the pros and cons of this type of management system, and explain their proposed LCMS solution.</p>

3. FUNCTIONAL REQUIREMENTS – MOBILE ID

High-level functional mobile ID requirements will be the focus of the mobile ID group. We will look to utilize the contemporary approach to requirements setting that has been successfully used as a best practice of peer agencies in the most recent procurement efforts. The goal of this approach is for the Contractor to identify, at a high-level, what functions we perform and require, and let the Contractors bring their solution for accomplishing those functions to bear in a proposal.

Mobile ID services use generally 10 or less than 10 finger data collected from subjects to launch searches of prior enrollments to determine whether the subject has been previously encountered and enrolled in the MBIS Solution.

3.1 OVERALL SERVICES CATEGORIES

- Mobile ID Services
 - Input
 - Processing
 - Outputs

This section addresses requirements relative to Mobile ID. Additionally, subsections here present how peer agencies address similar functions. Final subsections here allow for the approval of requirements to be promoted to the MBIS Solution RFP.

Table 12: Mobile ID TOT Supported

TOT	TRANSACTION NAME
RPIS	Rapid Print Image Search

3.2 MOBILE IDENTIFICATION SERVICES REQUIREMENTS

Mobile identification service specifications are organized under one of the three categories below:

- **Input** – The enrollment data will be transmitted as EBTS files originating at the mobile ID devices. These will be rapid turnaround transactions set to the highest priority, if not already set as such by the mobile ID device. At MBIS all records will be parsed for compliance with the EBTS. Transactions that fail the parsing test will be logged and returned to the submitting device with an ERRT response. Those transactions that comply will be forwarded to MBIS for response.
- **Processing** – The MBIS will process mobile transactions received from the field at the highest system priority level. The fingerprint images will be feature extracted and searched “without add.” Matcher results will be returned, where the results will be made available via EBTS responses. The transaction will be forwarded to the FBI for parallel searching against their RISC system.
- **Output** – The MBIS will prepare responses to all mobile ID transactions received. If the transaction failed to pass the various checks above, then it will have already produced an error message, pursuant to the EBTS. This section deals with requirements for successful transactions.

Table 13: Mobile Identification Services Requirements

ID	REQUIREMENT
INPUT	
MID Input 1	The MBIS SHALL be able to ingest mobile ID transactions and parse them for compliance with the EBTS to include checking for duplicate TCNs.
MID Input 2	The MBIS SHALL be able to forward the acceptable mobile ID transactions to the MBIS with the priority set to 1 (the highest priority value).
MID Input 3	The MBIS SHALL record in a log the results of each mobile ID transaction ingested.
MID Input 4	The MBIS SHALL store in a temporary file a copy of each mobile ID forwarded to the MBIS.
MID Input 5	The MBIS SHALL be able to ingest mobile ID transactions received from the various mobile ID devices.
MID Input 6	The MBIS SHALL record a copy of each ingested mobile ID transaction in a temporary file, configurable up to a year, in the ANSI/NIST Archive in the EBTS form in which it was received.
PROCESSING	
MID Proc 1	The MBIS SHALL process and search the fingerprint images and create an appropriate internal search of the matchers (TP-TP).
MID Proc 2	The MBIS SHALL automatically prepare and return an ERRT response containing the original TCN and Incident ID for all transactions that were not processable at the MBIS.
MID Proc 3	The MBIS SHALL automatically execute all TP-TP searches using the processed print in MID Proc 2.

ID	REQUIREMENT
MID Proc 4	If the matcher score for a technical candidate is above a settable threshold [Threshold 4], then the MBIS SHALL automatically send that positively identified subject to the device.
MID Proc 5	The MBIS SHALL forward transactions to the CalDOJ and/or FBI.
MID Proc 6	The MBIS SHALL ingest the FBI responses (RPISR and ERRT).
MID Proc 7	The MBIS SHALL automatically log to a searchable database all mobile ID search transactions results to include all subject and transaction information.
OUTPUT	
MID Output 1	If there is a positively identified subject, then the MBIS SHALL automatically return a response TOT to the device.
MID Output 2	If there are no candidates [MID Proc 3] available, then the MBIS SHALL automatically return a response TOT with that information.
MID Output 3	The MBIS SHALL automatically forward FBI responses (RPISR and ERRT) to the originating device.
MID Output 4	The MBIS SHALL be capable of automatically adding response transactions to the ANSI/NIST Archive.

4. FUNCTIONAL REQUIREMENTS – FACIAL ID

High-level functional Facial ID requirements will be the focus of the Facial ID group. We will look to utilize the contemporary approach to requirements setting that has been successfully been used as a best practice of peer agencies in the most recent procurement efforts. The goal of this approach is for the Contractor to identify, at a high-level, what functions we perform and require, and let the Contractors bring their solution for accomplishing those functions to bear in a proposal.

Facial ID services use generally Facial data collected from subjects to launch searches of prior enrollments to determine whether the subject has been previously encountered and enrolled in the MBIS Solution.

4.1 OVERALL SERVICES CATEGORIES

- Facial ID Services
 - Input
 - Processing
 - Outputs

This section addresses requirements relative to Facial ID. Additionally, subsections here present how peer agencies address similar functions. Final subsections here allow for the approval of requirements to be promoted to the MBIS Solution RFP.

Table 14: Facial ID TOT Supported

TOT	TRANSACTION NAME
IRQ	Facial Image Search

4.2 FACIAL IDENTIFICATION SERVICES REQUIREMENTS

Facial identification service specifications are organized under one of the three categories below:

- Input – The enrollment data will be transmitted as EBTS files originating at the Facial ID devices. These will be rapid turnaround transactions set to the configurable priority, if not already set as such by the Facial ID device. At MBIS all records will be parsed for compliance with the EBTS. Transactions that fail the parsing test will be logged and returned to the submitting device with an ERRT response. Those transactions that comply will be forwarded to MBIS for response.
- Processing – The MBIS will process Facial transactions received from the field at the configured system priority level. The Facial images will be feature extracted and searched “without add.” Matcher results will be returned, where the results will be made available via EBTS responses. The transaction can then be forwarded to CalDOJ.
- Output – The MBIS will prepare responses to all Facial ID transactions received. If the transaction failed to pass the various checks above, then it will have already produced an error message, pursuant to the EBTS. This section deals with requirements for successful transactions.

Table 15: Facial Identification Services Requirements

ID	REQUIREMENT
INPUT	
FID Input 1	The MBIS SHOULD be capable of ingesting Facial ID transactions and parse them for compliance with the EBTS to include checking for duplicate TCNs.
FID Input 2	The MBIS SHOULD be capable of forwarding the acceptable Facial ID transactions to the MBIS with the configurable priority set.
FID Input 3	The MBIS SHOULD be capable of recording in a log the results of each Facial ID transaction ingested.
FID Input 4	The MBIS SHOULD be capable of storing in a temporary file a copy of each Facial ID forwarded to the MBIS.
FID Input 5	The MBIS SHOULD be capable of ingesting Facial ID transactions received from the various Facial ID devices.
FID Input 6	The MBIS SHOULD be capable of record a copy of each ingested Facial ID transaction in a temporary (30 day) file in the ANSI/NIST Archive in the EBTS form in which it was received.
PROCESSING	
FID Proc 1	The MBIS SHOULD be capable of “feature extracting” the Facial images and create an appropriate internal search of the matchers.
FID Proc 2	The MBIS SHOULD be capable of automatically preparing and returning an ERRT response containing the original TCN and Incident ID for all transactions that were not processable at the MBIS.
FID Proc 3	The MBIS SHOULD be capable of automatically executing all Facial searches using the features extracted in FID Proc 1.
FID Proc 4	If the matcher score for a technical candidate is above a settable threshold [Threshold 4], then the MBIS SHOULD be capable of automatically adding that subject to the candidate list, in numerical ranking.
FID Proc 5	The MBIS SHOULD be capable of forwarding transactions to the CalDOJ and/or FBI.
FID Proc 6	The MBIS SHOULD be capable of ingesting the FBI responses.
FID Proc 7	The MBIS SHOULD be capable of automatically logging all Facial ID search transactions results to include the Type 1 fields, time received, time logged at end of processing, and the results.
OUTPUT	
FID Output 1	If there are any candidates (FID Proc 4) available, then the MBIS SHOULD be capable of automatically returning a response message with the five highest-scoring candidates and associated mug shots, if available.
FID Output 2	If there are no candidates [FID Proc 3] available, then the MBIS SHOULD be capable of automatically returning a response TOT with that information.

ID	REQUIREMENT
FID Output 3	The MBIS SHOULD be capable of automatically forwarding CalDOJ/FBI responses to the originating device.
FID Output 4	The MBIS SHOULD be capable of automatically adding response transactions to the ANSI/NIST Archive.

5. FUNCTIONAL REQUIREMENTS – IRIS ID

High-level functional Iris ID requirements will be the focus of the Iris ID group. We will look to utilize the contemporary approach to requirements setting that has been successfully been used as a best practice of peer agencies in the most recent procurement efforts. The goal of this approach is for the Contractor to identify, at a high-level, what functions we perform and require, and let the Contractors bring their solution for accomplishing those functions to bear in a proposal.

Iris ID services use generally 1 or 2 sets of iris data collected from subjects to launch searches of prior enrollments to determine whether the subject has been previously encountered and enrolled in the MBIS Solution.

5.1 OVERALL SERVICES CATEGORIES

- Iris ID Services
 - Input
 - Processing
 - Outputs

This section addresses requirements relative to Iris ID. Additionally, subsections here present how peer agencies address similar functions. Final subsections here allow for the approval of requirements to be promoted to the MBIS Solution RFP.

Table 16: Iris ID TOT Supported

TOT	TRANSACTION NAME
IRQ	Iris Image Search

5.2 IRIS IDENTIFICATION SERVICES REQUIREMENTS

Iris identification service specifications are organized under one of the three categories below:

- **Input** – The enrollment data will be transmitted as EBTS files originating at the Iris ID devices. These will be rapid turnaround transactions set to the configurable priority, if not already set as such by the Iris ID device. At MBIS all records will be parsed for compliance with the EBTS. Transactions that fail the parsing test will be logged and returned to the submitting device with an ERRT response. Those transactions that comply will be forwarded to MBIS for response.
- **Processing** – The MBIS will process Iris transactions received from the field at the configured system priority level. The iris images will be feature extracted and searched “without add.” Matcher results will be returned, where the results will be made available via EBTS responses. The transaction can then be forwarded to CalDOJ.
- **Output** – The MBIS will prepare responses to all Iris ID transactions received. If the transaction failed to pass the various checks above, then it will have already produced an error message, pursuant to the EBTS. This section deals with requirements for successful transactions.

Table 17: Iris Identification Services Requirements

ID	REQUIREMENT
INPUT	
IID Input 1	The MBIS SHOULD be capable of ingesting Iris ID transactions and parse them for compliance with the EBTS to include checking for duplicate TCNs.
IID Input 2	The MBIS SHOULD be capable of forwarding the acceptable Iris ID transactions to the MBIS with the configurable priority set.
IID Input 3	The MBIS SHOULD be capable of recording in a log the results of each Iris ID transaction ingested.
IID Input 4	The MBIS SHOULD be capable of storing in a temporary file a copy of each Iris ID forwarded to the MBIS.
IID Input 5	The MBIS SHOULD be capable of ingesting Iris ID transactions received from the various Iris ID devices.
IID Input 6	The MBIS SHOULD be capable of record a copy of each ingested Iris ID transaction in a temporary (30 day) file in the ANSI/NIST Archive in the EBTS form in which it was received.
PROCESSING	
IID Proc 1	The MBIS SHOULD be capable of “feature extracting” the iris images and create an appropriate internal search of the matchers.
IID Proc 2	The MBIS SHOULD be capable of automatically preparing and returning an ERRT response containing the original TCN and Incident ID for all transactions that were not processable at the MBIS.
IID Proc 3	The MBIS SHOULD be capable of automatically executing all iris searches using the features extracted in IID Proc 2.
IID Proc 4	If the matcher score for a technical candidate is above a settable threshold [Threshold 4], then the MBIS SHOULD be capable of automatically adding that subject to the

ID	REQUIREMENT
	candidate list, with any biometric-based strong candidate in the number one position.
IID Proc 5	The MBIS SHOULD be capable of forwarding transactions to the CalDOJ.
IID Proc 6	The MBIS SHOULD be capable of ingesting the FBI responses.
IID Proc 7	The MBIS SHOULD be capable of automatically logging all Iris ID search transactions results to include the Type 1 fields, time received, time logged at end of processing, and the results.
OUTPUT	
IID Output 1	If there are any candidates (IID Proc 4) available, then the MBIS SHOULD be capable of automatically returning a response TOT with the five highest-scoring candidates and associated mug shots, if available.
IID Output 2	If there are no candidates [IID Proc 3] available, then the MBIS SHOULD be capable of automatically returning a response TOT with that information.
IID Output 3	The MBIS SHOULD be capable of automatically forwarding CalDOJ/FBI responses to the originating device.
IID Output 4	The MBIS SHOULD be capable of automatically adding response transactions to the ANSI/NIST Archive.

6. TECHNICAL AND STANDARDS REQUIREMENTS

This section provides the system technical requirements for the new MBIS environment. The technical requirements (also known as non-functional requirements) are organized as follows:

- Capacity requirements – capability to store some number of a class of items such as:
 - Enrolled transactions.
 - Searchable feature-based data sets online in matchers.
- Performance requirements – number of events and units of time such as:
 - Throughput as expressed in transactions turned around in a period of time.
 - Average transaction response time.
- Accuracy requirements – matcher capability.
 - Tenprint to tenprint accuracy.
 - Tenprint to latent accuracy.
 - Latent to tenprint accuracy.
 - Palm latent to known palm accuracy.
 - Criminal known palm to latent accuracy.
- Safety requirements.
- Security requirements.
- Environmental requirements – such as uninterruptible power supplies (UPSs) and office environment noise levels

- Hardware requirements – capacities and performance of workstations and printers.
- Backup/Recovery/Availability requirements.

6.1 STORAGE CAPACITY REQUIREMENTS

Storage capacities are relevant to the following areas of the MBIS system architecture, including:

- ANSI/NIST Archive.
- The templates/features loaded in the matchers.

The following subsections delineate these requirements and will refer to the tables provided below.

Table 18: Annual System Metrics

RECORD TYPE	2009	2010	2011	2012	GROWTH RATE
Registered MAIN Numbers	3,896,801	4,021,159	4,141,491	4,234,079	2%
Records in NIST Archive	3,480,469	3,859,862	4,223,479	4,588,630	2%
Ten-Print Searches	408,685	451,997	369,497	357,941	2%

Table 19: Current LACRIS Record Counts

LACRIS RECORD TYPE	OCTOBER 2012	JANUARY 2013
Ten-Prints	11,740,616	11,885,223
MAIN Subjects	4,336,089	4,372,098
Palm Prints	N/A	2,257,182
Unsolved Latent	233,882	240,025
Unsolved Palm Latent	92,137	95,580

The MBIS will be designed to accommodate an ANSI/NIST Archive of all input and output transactions through the term of the Agreement. The addition of response TOTs will make the capacity requirements larger than the storage of input transactions only. Note that most response transactions generated by the MBIS are smaller than the corresponding input transactions. The Contractor will have to perform the appropriate design analysis to determine the design requirements in terms of terabytes as a function of transaction type using the data specified in this document.

At the initial operating point of the MBIS, all existing records will have been loaded into the MBIS, to include loading them into the ANSI/NIST Archive, the matchers, any other repositories, and the master index.

The MBIS storage requirements are listed in the table below.

Table 20: MBIS Storage Capacity Requirements

REQUIREMENT ID	REQUIREMENT
Stor Req 1	The MBIS SHALL have the capacity to store in the ANSI/NIST Archive at the beginning of any year, at least the number of EBTS transactions listed per year in the tables above for that year.
Stor Req 2	The MBIS SHALL have the annual capacity to store in the matchers the templates for enrolled fingerprints.
Stor Req 3	The MBIS SHALL have the annual capacity at the beginning of the year to store in the matchers the templates for enrolled unsolved fingerprints and palmprints at the levels shown in the tables.
Stor Req 4	The the MBIS SHALL have the capacity to store a backup copy on portable digital media of all ANSI/NIST transactions that are in the ANSI/NIST Archive and the biometric feature sets (also known as templates) in the matchers, in any given year, as a backup for the Archive and matchers.
Stor Req 5	The MBIS SHALL have the capacity and ability to create and store MBIS level logs for all activities listed in the Functional Requirements for a period commensurate with the FBI CJIS Security Policy, version 5.0, plus 3 additional years.

6.2 PERFORMANCE REQUIREMENTS

The MBIS will meet performance (throughput and response time) requirements as specified in this section.

6.2.1 THROUGHPUT REQUIREMENTS

The MBIS throughput requirements cover all three of the primary current types of services:

- Tenprint services.
- Latent services.
- Mobile ID services.

The MBIS throughput rates will grow over the life of the system – The following table projects the growth for the term of the Agreement.

Table 21: Annual LACRIS Transaction Counts

TRANSACTION TYPE	2010	2011	2012	GROWTH RATE
CRM	373,436	350,924	327,197	2%
CUS	0	0	0	2%
REG	5,085	6,427	8,840	2%
SUP	0	0	0	0
COR	0	0	0	0
IDN	41,137	23,444	12,646	2%
IDN2	916	0	0	2%
IDN4	306,073	392,822	339,629	10%
APP	1	1	0	2%
Latent	44,289	54,179	58,737	2%
Palm Latent	18,023	27,803	29,023	2%
TLI	<u>382,409</u>	<u>363,730</u>	<u>345,118</u>	2%
Total	1,171,369	1,219,330	1,121,190	

Legend:

- CRM – criminal booking.
- CUS – custody TOT, this is for the inmate realignment. State prisoners being moved to counties.
- REG – registrant TOT.
- SUP – supplemental.
- COR – coroner, deceased.
- IDN – identification transaction, state transaction, full roll.
- IDN2 – county ID transaction, two index fingers.
- IDN4 – county ID transaction, flats (four finger and thumbs).
- APP – applicant (not retained in our AFIS, passed through to DOJ).
- Latent – latent search.
- Palm Latent – palm latent.
- TLI – ten-print to latent ID.

The throughput requirements are defined in the table below. Throughput requirements are for concurrent ingestion and processing of identification, forensic, and tactical transactions.

Table 22: Throughput Requirements

REQUIREMENT ID	REQUIREMENT
ThruPut Req 1	The MBIS SHALL be able to ingest, process, and respond in the peak period to at least the daily average of transaction counts noted in the table above while maintaining the response times noted in the table below, while latent and Mobile ID transactions are being ingested, processed, and responded to. [This requirement is independent of any time for examiners to perform QC on the input stream or to review candidate lists/perform verification.]
ThruPut Req 2	The MBIS SHALL be able to ingest, process, and respond in the peak period to at least the daily average of transaction counts noted in the table above while maintaining the response times noted in the table below, while identification and Mobile ID transactions are being ingested, processed, and responded to. [This requirement is independent of any time for examiners to perform QC on the input stream or to review candidate lists/perform verification.]
ThruPut Req 3	The MBIS SHALL be able to ingest, process and respond in the peak period to at least the daily average of transaction counts noted in the table above while maintaining the response times noted in the table below, while identification and latent transactions are being ingested, processed, and responded to.
ThruPut Req 4	If in any day the MBIS is presented with more transactions in a peak hour than the design capacity, then the MBIS SHALL queue the additional work and process it as soon as capacity is available, with that processing to be based on the priority of the transactions.

6.2.2 RESPONSE TIME REQUIREMENTS

The Response Time for MBIS transactions is a function of the transaction type (identification, forensic, and tactical [Mobile ID]). The Response Times do not include any human interaction times.

The table below provides the response times per class of transaction, while the Response Time Requirements table defines the requirements for providing these response times.

Table 23: Response Times Per Transaction Type

TRANSACTION CLASS TYPES	RESPONSE REQUIREMENTS UNDER PEAK LOAD
Criminal TP-TP	1 minute
TP-LT	1 minute
LT-TP	1 minute
Palm LT-KP	10 minutes
Criminal KP-LT	5 minutes
Mobile ID TP-TP	30 seconds

The response time requirements stated below are for 95 percent of the transactions in any period, as there are always some outliers caught up in a data processing system and they should not be considered in the performance testing. Testing will be done against the initial repository load using a test set with a mixture of all transaction types at the peak rates calculated using the table above.

Table 24: Response Time Requirements

REQUIREMENT ID	REQUIREMENT
Response Req 1	<p>The MBIS SHALL provide responses for 95 percent of submitted transactions in accordance with the response times noted in the table above.</p> <p>Response time to be measured from the end of ingest through the final response, to the return of a response from the MBIS to the submitting device with no error TOTs in the mix.</p>
Response Req 2	<p>The MBIS SHALL use transaction priority in assigning transactions to queues and in processing them when higher than peak transaction rates are encountered – processing higher priority transactions ahead of lower priority transactions in the same Transaction Class Type.</p>

6.3 ACCURACY REQUIREMENTS

The matcher accuracy will vary as a function of the class of service (identification, forensic, and tactical (Mobile ID) and the quality of the input images. Identification service accuracy requirements are typically higher than those for forensic services, as the input images are typically of better quality for Live-Scan enrollments than for latent lifts.

Accuracy terms-of-art have been undergoing an evolutionary change for the past few years. While reliability, true accept rate, false reject rate, and other terms are often used for access control systems and other biometric modalities (such as facial recognition) – a consensus has developed in the international standards community around the terms *true match rate* and *failure to match rate* when discussing friction ridge matching on a large scale.

For this project accuracy will include three accuracy terms:

- *True Match Rate* – the probability that a true match will be found when it is in the background reference file (also known as a repository). This term replaces older terminology such as matcher reliability or true accept rate.
- *Failure to Match Rate* – the probability that a search will not return a true match when the true match is in the reference file. The failure to match rate is 100 percent minus the true match rate. While not explicitly stated in the requirements, it will be calculated during testing and reported.
- *Selectivity* – the number of candidates that will be examined to determine the true match rate. While the system administrators will be able to selectively change the length of candidate lists by transaction class, and by threshold scores, during testing, system accuracy will be measured using the selectivity numbers shown in the table that follows.

Table 25: Accuracy Rates by Transaction Type

TRANSACTION TYPES	SELECTIVITY	TRUE MATCH RATE
TP-TP	1	99.9%
Mobile ID TP-TP (with fewer than 10 prints)	8	99.9%
TP-LT	10/25	93%/100%
Criminal KP-LT	10/25	93%/100%
LT-TP	10/25	93%/100%
Palm LT-KP	10/25	93%/100%

The accuracy requirements are listed in the following table.

Table 26: Accuracy Requirements

REQUIREMENT ID	REQUIREMENT
Accuracy Req 1	<p>The MBIS SHALL provide accuracy for submitted transactions in accordance with the values in the table above while conforming to the response times in noted in the table above.</p> <p>The accuracy will be measured using Contractor best practices.</p>

6.4 SAFETY REQUIREMENTS

There are two requirements for the electrical safety of the MBIS. They are specified in the following table. The intent is to ensure that safe equipment is used and that it is installed properly in terms of grounding (e.g., any power strips used at the MBIS workstations must be certified and be installed and used correctly).

Table 27: Safety Requirements

REQUIREMENT ID	REQUIREMENT
Safety Rqt 1	All hardware configuration items delivered as part of the MBIS SHALL conform to the appropriate U.S. Underwriters Laboratory standards for electronic devices and be so certified.
Safety Rqt 2	All required grounding SHALL conform to the manufacturer's specifications and recommendations.

6.5 SECURITY REQUIREMENTS

All configuration items that process, transmit, or store digital information delivered as part of the MBIS will require some level of InfoSec, as the system is connected to local, state and federal criminal justice networks. All Los Angeles County Sheriff's Department, Los Angeles County, state and federal information security must be complied with including user and administrator login rules, audit trail requirements, and reporting capabilities.

InfoSec includes ensuring data confidentiality, integrity, and availability – and thus antivirus protection is to be included in the systems to the extent to which there are commercial antivirus packages available for the operating systems selected by the Contractor. The InfoSec requirements are listed below.

Table 28: InfoSec Requirements

REQUIREMENT ID	REQUIREMENT
InfoSec Req 1	The MBIS design SHALL conform to Los Angeles County Sheriff's Department, Los Angeles County information security and the CJIS Security Policy v5.0 or later.
InfoSec Req 2	Antivirus software SHALL be loaded on all processors that run operating systems where there are commercial antivirus packages available.
InfoSec Req 3	The antivirus software SHALL automatically virus scan all files on portable data storage devices (i.e., CDs, DVDs, USB devices with memory, and floppy disk media) presented to a system and report alerts and other problems.
InfoSec Req 4	The antivirus software SHALL automatically log all virus alerts and action taken.
InfoSec Req 5	The MBIS SHALL support the updating of antivirus software databases of virus information without compromising the security of the system.

6.6 ENVIRONMENTAL REQUIREMENTS

There are MBIS imposed environmental requirements on all workstations and workstation peripherals such as printers.

The system design will include the capability to meet the following power/voltage conditioning and related availability requirements as well as noise level requirements as noted in the table below. These requirements address sustainment of power during blackouts and brownouts and noise levels in an office environment.

Table 29: Environmental Requirements

REQUIREMENT ID	REQUIREMENT
Envrn Req 1	Each workstation SHALL have a UPS that can support the workstation for up to 20 continuous minutes in the event of a loss of building power.
Envrn Req 2	Each workstation UPS SHALL provide the user with a signal in cases where the UPS has been the only source of power to the device for 10 continuous minutes.
Envrn Req 3	Each workstation SHALL automatically shut down properly, based upon the receipt of a 10-minute warning, if the operator does not initiate a shutdown

REQUIREMENT ID	REQUIREMENT
	within 10 minutes of the signal when the UPS has continuously remained the only source of power to the device for that time.
Envrn Req 4	<p>The verification stations SHALL be able to operate in an office environment, without any requirement for supplemental air conditioning or noise suppression:</p> <ul style="list-style-type: none"> • 68° to 72° temperature with a relative humidity between 40 and 60 percent. • Noise below 70 dBA measured at the workstation suite.

6.7 HARDWARE REQUIREMENTS

This section provides the form and fit requirements for the MBIS as indicated in the table below. The requirements are for the workstations and card printers to be delivered to MBIS sites, to include the locations and number of units per site.

Table 30: Hardware Requirements for Workstations and Printers

REQUIREMENT ID	REQUIREMENT
Hdwe Req 1	<p>All workstations SHALL be core configured to be capable of running or functioning as either, excepting peripheral equipment, a tenprint or latent workstation. Specifically, each tenprint workstation SHALL minimally have:</p> <ul style="list-style-type: none"> • A microprocessor with at least 3.2 GHz clock speed and at least four cores. • Built in graphics or a graphics board with at least 1 GB of onboard memory. • 8 GB of internal RAM. • One 25-inch or larger flat panel display with at least 1920×1200 resolution and digital visual interface. • 1 Gigabit Network Interface Card. • At least one 750 GB hard disk drive. • Keyboard and mouse. • FBI EBTS Appendix F certified flatbed scanner. • The most recent version of the operating system that was used to certify the scanner. • A full suite of the Contractor tenprint software, and the ability to use the Contractor latent software.
Hdwe Rqt 2	<p>All workstations SHALL be core configured to be capable of running or functioning as either, excepting peripheral equipment, a tenprint or latent workstation. Specifically, each latent workstation SHALL minimally have:</p> <ul style="list-style-type: none"> • A microprocessor with at least 3.2 GHz clock speed and at least four cores. • Built in graphics or a graphics board with at least 1 GB of onboard memory. • 8 GB of internal RAM. • Two 25-inch or larger flat panel displays with at least 1920×1200 resolution and digital visual interface. • 1 Gigabit Network Interface Card. • At least one 750 GB hard disk drive. • Keyboard and mouse. • FBI EBTS Appendix F certified flatbed scanner.

REQUIREMENT ID	REQUIREMENT
	<ul style="list-style-type: none"> • The most recent version of the operating system that was used to certify the scanner • Adobe Photoshop Elements™ Version 9 or later. • A full suite of the Contractor latent software, and the ability to use the Contractor tenprint software.
Hdwe Rqt 3	<p>Each administrative workstation SHALL minimally have:</p> <ul style="list-style-type: none"> • A microprocessor with at least 3.2 GHz clock speed and at least four cores. • Built in graphics or a graphics board with at least 1 GB of onboard memory. • 8 GB of internal RAM. • One 25-inch or larger flat panel display with at least 1920×1200 resolution and digital visual interface. • 1 Gigabit Network Interface Card. • At least one 750 GB hard disk drive. • Keyboard and mouse. • The most recent version of the operating system that was used to certify the scanner • Microsoft Office™ Version 2010 or later.
Hdwe Rqt 4	<p>Each card printer SHALL minimally have:</p> <ul style="list-style-type: none"> • At least two drawers/trays to support fingerprint and palmprint card stock simultaneously without having to physically change trays. • FBI Appendix F Certification. • Connectivity to a workstation or server running the most recent version of the operating system that was used to certify the printer • Simultaneous two-sided print capability. • 1 Gigabit Network Interface Card. • At least 256 MB of memory.
Hdwe Rqt 5	<p>The mugshot system SHALL have the highest possible resolution camera for facial identification and examination.</p>

6.8 BACKUP/RECOVERY/AVAILABILITY REQUIREMENTS

This section provides the backup/recovery/availability requirements for the MBIS. To support these, there are requirements for the ability to backup and restore the system or any of its major data components.

There are two sets of requirements:

- Backup and recovery.
- Availability and restoration.

6.8.1 BACKUP AND RECOVERY

The MBIS will need to be backed up (data and system configurations) frequently for Continuity of Operations considerations. Copies of the backup tapes will be stored off site from the central site (Primary Site and Disaster Recovery Sites) to increase the likelihood of their availability in case of a natural or man-made disaster. These backup files will be created and moved off site. The requirements for backup and recovery are listed in the table below.

Table 31: Backup and Recovery Requirements

REQUIREMENT ID	REQUIREMENT
Backup Req 1	The MBIS SHALL permit the Contractor system administrators to selectively create full and incremental SAN-based backups of any or all files on the MBIS, to include administrative files, ANSI/NIST Archive files, transaction files, master identity indexes, transaction results, and the back-end matcher files, to include feature sets and matcher identity indexes, without impacting functionality of the system.
Backup Req 2	The MBIS SHALL permit the Contractor system administrators to selectively support the recovery of any or all files from the backups [BackupReq 1] to the appropriate locations.
Backup Req 3	The MBIS SHALL maintain synchrony between the primary MBIS site and the disaster recovery site such that each and every transaction successfully enrolled in the operational site is still available in case of a switchover to the other MBIS site.

6.8.2 SERVICE AVAILABILITY AND RESTORATION REQUIREMENTS

Given that the MBIS will operate under a COOP to include a Disaster Recovery Site, it is anticipated that MBIS services will have a very high level of continuous availability.

- The availability of all MBIS services (Service Availability) is set at 99.8 percent per month without any allowance beyond 99.8 percent for scheduled outages or switchover from the Primary Site to the Disaster Recovery Site (or vice versa). Service Availability of 99.8 percent leaves a little less than 90 minutes a month for service outages at the MBIS level. The Contractor is free to roll scheduled outages between the Primary Site and Disaster Recovery Sites to preclude as many MBIS service outages as possible. The purposes of the Disaster Recovery Site are to:
 - Provide for fast recovery for failed equipment and localized power outages at the primary site – 99.8 percent availability is a requirement. This includes provision of any and all necessary power conditioning and alternative power sourcing to maintain the Service Availability Requirement.
 - Provide the basis for recovery of services in the event of a catastrophic failure at the Primary Site (fire, explosion, radioactive contaminations, etc.).

The requirements for Service Availability (Service Availability Requirements) are listed in the table below.

Table 32: MBIS Availability Requirement

REQUIREMENT ID	REQUIREMENT
SAR Req 1	<p>The MBIS SHALL provide at least 99.8 percent Service Availability of all MBIS services unless a catastrophic event occurs – measured monthly, to include as unavailable time (1) any scheduled outages for preventive maintenance and (2) planned upgrades where the MBIS users do not have access to and the use of MBIS services.</p> <p>For purposes of this requirement “catastrophic event” is defined as a natural or man-made disaster that destroys both the MBIS Primary Site and Disaster Recovery Sites or renders both unusable due to fire, water damage, earthquake, radioactive leak, large-scale power outage, declared medical pandemic, or a large-scale communications infrastructure outage (telephones and Internet access). Large-scale means at least impacting the city where the site is located.</p>

6.9 INTERFACE REQUIREMENTS

The key interfaces/exchanges operational and required in the LACRIS environment are described in the table below.

Table 33: Interface Requirements

REF.	INTERFACE/EXCHANGE
1	<i>CAL-DOJ Automated Fingerprint Identification System (AFIS)</i> – The California Identification System (CAL-ID) is the AFIS managed by the CAL-DOJ. LAFIS forwards all fingerprint transactions to CAL-ID by FTP and Web Services, after local processing is completed.
2	<i>FBI IAFIS</i> – IAFIS is operated and managed by the FBI. Currently, ten-print transactions are automatically forwarded to FBI IAFIS by CAL-ID.
3	<i>County Live-Scan System</i> – The county's Live-Scan system is the ten-print data source (initial input devices) for LAFIS. Live-Scan communicates with LAFIS by FTP. LAFIS communicates with Live-Scan by e-mail.
4	<i>Countywide Warrant System (CWS)</i> – LAFIS has the ability to communicate with Los Angeles County's CWS through the county's Justice Data Interface Controller (JDIC) using TCP/IP.
5	<i>County Automated Justice Information System (AJIS)</i> – AJIS maintains arrest, booking, and custody information for offenders in Los Angeles County. Currently, AJIS receives its positive fingerprint-based identifier (MAIN #) from the LAFIS.
6	<i>County Mug Shot System</i> – Los Angeles County Photo Manager (LAPM) is the county repository for mug shot images. LAFIS supplies LAPM with positive ID matches against the LAFIS database through FTP and a tickle table.
7	<i>Mobile ID</i> – This allows access by mobile identification devices to LAFIS from the field, for the submission of inquiries, and the return of responses. Transactions are managed through the Contractor's proprietary Web page.

The interface requirements are listed in the following table.

Table 34: Interface Requirements

REQUIREMENT ID	REQUIREMENT
Interface Req 1	The MBIS SHALL provide, test and implement each and all of the interfaces listed in the table above during implementation of the new system environment.

6.10 STANDARDS REQUIREMENTS

The current standards and models applicable operational and required in the current LAFIS environment include:

- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- Electronic Biometric Transmission Specification (EBTS), IAFIS-DOC-01078-9.4.
- IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- NIST Best Practice Recommendation for the Capture of Mugshots. Version 2.0. September 23, 1997.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.0, CJIS Security Policy, Version 5.0, dated February 9, 2011.

The standards requirements are listed in the following table.

Table 35: Standards Requirements

REQUIREMENT ID	REQUIREMENT
Standards Req 1	The MBIS SHALL be compliant with each and all of the standards listed in the table above in the new system environment.

6.11 ADMINISTRATIVE FUNCTIONS REQUIREMENTS

The system administrators (Contractor staff and LACRIS staff) will be responsible for the integrity of information in the system; creating and maintaining user accounts; exporting files in response to ad-hoc requests; and generating reports, as appropriate.

In addition to the normal Administrative tasks described further below, there is one added set of requirements associated with testing new and modified TOTs.

Administrative Function service specifications are organized under one of the three categories below:

- **Input** – System administrators use this workflow to test new and modified TOTs. The TOTs can be any of those ingested by or created as output by any other workflow. They may be sent to the MBIS. The format is the normal TOT name with a T appended to it (***T) to signal all systems that it is a test transaction and thus should not be added to any system.
- **Processing** – The MBIS will process locally all test transactions received.
- **Output** – The MBIS will prepare responses to all test transactions received. The requirements are listed in the table below.

This table lists the TOTs associated with this requirement.

Table 36: Test Transaction TOTs Supported

TYPE OF TRANSACTION	TRANSACTION NAME
***T	Test Transaction version of any Workflow TOT

All Test transactions will be parsed for compliance with the MBIS EBTS. Transactions that fail the parsing test will be logged and returned with an ERRT response. Successful transactions (i.e., those that pass the parser checks) will be forwarded to the originator.

Table 37: Test Transaction Input Requirements

REQUIREMENT ID	REQUIREMENT
INPUT	
Test Input 1	The MBIS SHALL be able to ingest test EBTS transactions from any criminal record repository and parse them for compliance with the MBIS EBTS, to include checking for duplicate TCNs.
Test Input 2	The MBIS SHALL be able to respond to the noncompliant Test transactions via an EBTS error transaction (ERRT) to the criminal record repository or other submitter.
Test Input 3	The MBIS SHALL be able to forward the acceptable Test transactions to the originator.
Test Input 4	The MBIS SHALL record in a log the results of each Test EBTS ingested.
Test Input 5	The MBIS SHALL be able to ingest Test EBTS transactions received from the various devices.
PROCESSING	
Test Proc 1	The MBIS SHALL process the test EBTS transactions received from the devices and process them
Test Proc 2	The MBIS SHALL process the test transaction – without adding or changing the archive, the matcher repositories, or any indexes.
Test Proc 3	The MBIS SHALL update the transaction log with the processing results.
OUTPUT	
Test Output 1	The MBIS SHALL automatically generate and forward the appropriate system response transaction to the submitting criminal record repository.
Test Output 2	If the Test Transaction is marked to be forwarded to the FBI, the MBIS SHALL automatically forward it as designated during the system design.
Test Output 3	The MBIS SHALL ingest all responses received from the FBI and forward them to the appropriate device.
Test Output 4	The MBIS SHALL update the transaction log with the processing results.

Administrative tasks will start with a system administrator logging into a workstation connected to MBIS. The system administrators will deal with system error messages, assist in recovering from problems, and generate problem reports via e-mail, 24/7 help desk calls, or other means.

Table 38: System Administrator Input Requirements

REQUIREMENT ID	REQUIREMENT
Admin Function 1	The MBIS SHALL permit the system administrators to selectively set up and manage at least 10 classes of users (e.g., latent supervisor) with configurable permissions per class.
Admin Function 2	The MBIS SHALL support the system administrator in assigning workflows and within workflows specific TOTs to default priority queues – with up to 9 priorities to conform to the ANSI/NIST Standard for Field 1.006: <i>“The values shall range from “1” to “9”, with “1” denoting the highest priority. The default value shall be defined by the agency receiving the transaction.”</i>
Admin Function 3	The MBIS SHALL support the system administrator in maintaining and changing Thresholds 1, 2, 3, and 4 as appropriate.
Admin Function 4	The MBIS SHALL support the system administrator in maintaining and changing QC thresholds for tenprints and separately for palmprints.
Admin Function 5	The MBIS SHALL support the system administrator in maintaining and changing default candidate lengths for verification, separately for tenprints, forward latents, and reverse latents.
Admin Function 6	The MBIS SHALL support the system administrator in maintaining and changing a selectable second-level verification per International Standards Organization (ISO) standards.
Admin Function 7	The MBIS SHALL support the system administrator in selectively reviewing and printing the MBIS logs – reviewing and printing may be organized by any or all of the following: time, date, user, transaction type, file-accessed name, device logged into, problem reports, transaction control number, and transaction results.
Admin Function 8	The MBIS SHALL enable the system administrator to selectively back up IT, biographic, ANSI/NIST archive, and forensic files at all system levels from workstations to the MBIS.
Admin Function 9	The MBIS SHALL support the system administrator in selectively restoring IT, biographic, ANSI/NIST Archive, and forensic files.
Admin Function 10	The MBIS SHALL allow the system administrator to selectively ingest any supported transactions, individually or in bulk, and process them as appropriate to the TOT.
Admin Function 11	The MBIS SHALL permit the system administrator to selectively cancel programs that are not responding and restart any program or computer.
Admin Function 12	The MBIS SHALL support the forensic system administrator in selectively exporting “known” files in bulk or individually.
Admin Function 13	The MBIS SHALL support the system administrator in selectively exporting

REQUIREMENT ID	REQUIREMENT
	“unknown” (latent) files in bulk or individually.
Admin Function 14	The MBIS SHALL support the systems administrator in preparing selective reports for, at a minimum, selectable (1) time periods (2) classes of services, and on use patterns of the MBIS and aggregating those reports so they can be edited, merged with other reports, and printed.
Admin Function 15	<p>The MBIS SHALL support automated logging and system administrator selective reporting on the following information:</p> <ul style="list-style-type: none"> • General central system monitoring • Use by time, person, functionality, etc. • Viruses encountered – at the device level. • All events associated with unsuccessful login attempts, at the device level.
Admin Function 16	<p>The MBIS SHALL support automated logging and system administrator selective reporting on the following information:</p> <ul style="list-style-type: none"> • Disk memory used, free, and as-built totals by system and component: <ul style="list-style-type: none"> ▪ ANSI/NIST Archive. ▪ Temporary files. ▪ The LCMS. • Matcher memory used, free, and totals by system, by component, and by modality (e.g., reverse palm search matchers).
Admin Function 17	<p>The MBIS SHALL support automated logging and system administrator selective reporting on the following information:</p> <ul style="list-style-type: none"> • A record of abnormal shutdown of any computer, along with any available diagnostics. • Number and percentage of transactions by class that failed/passed parser and image quality checks.
Admin Function 18	<p>The MBIS SHALL support automated logging and system administrator selective reporting on the following information:</p> <ul style="list-style-type: none"> • NFIQ scores by finger, TOT, ORI, and/or time.
Admin Function 19	<p>The MBIS SHALL support automated logging and system administrator selective reporting on the following information:</p> <ul style="list-style-type: none"> • Number of transactions, searches by class, hit rate by class, hit rate by TOT, error rate in processing transactions, and current size of each repository to include available space, selectively for one or more system elements, or the entire MBIS.
Admin Function 20	The MBIS SHALL support the selective production of reports from all workflows and administrative functions to a specified color or gray-scale printer; to a file using comma-separated format for future use to include editing and merging with other such files; and saving reports as an Adobe Portable Data Format (PDF) file; to include the list of reports that follows this table.

REQUIREMENT ID	REQUIREMENT
Admin Function 21	The MBIS SHALL offer MBIS management the ability to easily track, monitor and produce reports on the types of tenprint, latent, and administrative activities listed below this table.
Admin Function 22	The MBIS SHALL permit administrators to design their own report formats from pull-down menus.
Admin Function 23	The MBIS SHALL permit administrators to synchronize system time across all MBIS elements that have or use time clocks (e.g., servers, workstations, and logs).
Admin Function 24	The MBIS SHALL permit administrators to select auto synchronization of system time across all MBIS elements that have or use time clocks (e.g., servers, workstations, and logs) on a selectable frequency (between 6 hours and 24 hours).
Admin Function 25	The MBIS SHALL support a dedicated test site that could be used as a training site facility in the new environment.

Reports

The following types of reports are associated with Admin Function 20:

- Transactions processed on MBIS to include ability to select from the following display options *by workflow and TOT*:
 - Number of transactions received and processed.
 - Number of hit/no hit transactions.
 - Number of transactions sent to CalDOJ and/or FBI (and other national databases), number of responses received, percentage of responses that were hits.
 - Number of transactions by day/week/month/quarter/year and average hour versus peak hour.
 - Number of transactions processed by crime type.
 - Selectable date ranges.

The MBIS **SHALL** support the latent examiners and system administrators in selectively reporting on latent case management status over the life of the system or any selected shorter period of time to include at a minimum:

- Number of open and closed cases.
- Number of cases closed due to a match.
- Expiration of associated data due to statute of limitations or other reasons.
- Average number of latent images per open case.
- Maximum number of latent images per case.
- Percentage of capacity used at various levels.
- Number of cases within 90, 60, and 30 days of eclipsing their associated statute of limitations.
- Average number of minutiae per latent finger or palm.

- Maximum and minimum number of minutiae per latent finger or palm.
- Number of searches executed.
- Average number of searches executed per latent image.

In addition the MBIS **SHALL** allow the MBIS system administrator to generate reports on capacities and sizes to include, by selectable date:

- Criminal, ID slaps, and/or tactical submissions by:
 - Number of individuals in databases and/or archives by tenprint, known palms, unknown palms, and unsolved latent records.
 - Number of fingers in databases and/or archives by tenprint, known palms, facial images, and unsolved latent records (fingerprints and palmprints).
 - Sex of individuals in databases and/or archives by tenprint, known palms, and facial images.
 - Average image quality (using NFIQ and Contractor metrics) for rolled fingerprints and flats for databases or archives by finger and averaged across both hands.
- For databases, archives, and matchers:
 - Sizes and usage by selectable date.
 - Capacity available by selectable date.
 - Projected need for additional capacity by date.
- Administrative reports for each MBIS matcher, to include at a minimum:
 - Matcher number and name – types of data contained in the matcher.
 - Number of Individuals enrolled in each matcher.
 - Number of individuals with one record, two records, or three records in the matcher.
 - Average minutiae per record.
 - Average NFIQ score per finger per image.
 - Average compression rates per image.
- Administrative reports for all of MBIS reflecting the following information, at a minimum:
 - Number of persons authorized to access the MBIS.
 - Number of persons who have administrator access.
 - Number of persons who have tenprint access.
 - Number of persons who have latent print access.
 - Number of Live-Scans.
 - Number of ORIs .
 - Number of workstations (by type).

7. QUALIFICATION REQUIREMENTS

This section establishes requirements for formal verification of the design and performance requirements set forth in Section 6.3 (Accuracy Requirements) of these Specifications.

7.1 VERIFICATION METHODS

The specified methods of verification are inspection, analysis, demonstration, and test, as well as productive combinations of these methods. These methodologies are defined below:

7.1.1 INSPECTION

Inspection shall verify through visual means, physical manipulation, gauging, or measurement that specified requirements have been met. For software, inspection includes physical examination of documentation, a listing of program code, or both to verify conformance to specified requirements.

7.1.2 ANALYSIS

Analysis shall verify that the item meets specified requirements by technical evaluation of equations, charts, graphs, models, diagrams, and representative data, or by evaluation of previously qualified equipment and software to equivalent or more stringent criteria.

7.1.3 DEMONSTRATION

Demonstration shall verify that the item meets specified requirements by operation, manipulation, or adjustment of the item to produce a correct operational state for the item. Instrumentation (e.g., code) and monitoring may be used to verify attainment of the specified operational state.

7.1.4 TEST

Test shall verify that the item meets specified requirements by use or operation of the item with instrumentation to record quantitative data, and by comparison of the resultant quantitative data with established quantitative standards or criteria. Test differs from demonstration in the measurement of quantitative data and the comparison of results to predicted criteria. Any requirement that does not contain a measurable item will not be verified by test.

7.2 VERIFICATION CONDITIONS

Verification conditions are specific conditions under which the requirement **SHALL** be verified. For testing of accuracy and response time requirements, the following conditions will be set.

The converted repositories (known and unknown friction ridge files as well as related feature sets, pointers, and tables) will be audited as part of the central site acceptance testing (AT). Accuracy tests will employ these repositories, while the search records will be data sets prepared by MBIS and having known image quality (tenprint only), minutiae counts (latents and their mates only) and mate or no-mate status information. AT will include two accuracy tests: one with minimal human intervention (known as lights out) and one with expert human intervention following the Contractor's recommended best practices. There will be appropriate levels of performance required for each of these two accuracy tests.

The first table below shows the anticipated parameters for AT accuracy matching, with examiner assistance limited to orientation of latent images and marking the boundary (a.k.a. the region of interest) of the latent image area to be searched. This is referred to as lights out accuracy testing. The second table below shows the anticipated parameters for best practices accuracy matching.

Table 39: Lights Out Accuracy Verification Conditions

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Search Records	10,000	10,000 ¹	200	5,000	100
Mated Records	50%	100	100	10	40
NFIQ Average of Mated TPs	3.1 or Better	3.1 or Better	3.1 or Better	N/A	N/A
Minimum Number of Simultaneous Minutiae of Mated Items	N/A	16	16	16	16
Selectivity ²	1	10/25	10/25	10/25	10/25
True Match Rate ³	99.8%	45%/60%	45%/60%	45%/60%	45%/60%
Non-Mated Search Records	50%	9,900	100	4,990	60
Background Repository	All Converted TP Records	All Converted LT Records	All Converted TP Records	All Converted Palm LT	All Converted KP Records

1 – These transactions will be cascaded from the 10,000 TP-TP searches.

2 – Selectivity is a measure of allowed candidate list length.

3 – Assumes a true match is in the searched file.

Table 40: Best Practices Accuracy Verification Conditions

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Search Records	10,000	10,000	200	5,000	100
Mated Records	50%	100	100	10	40
NFIQ Average of Mated TPs	1	1	1	N/A	N/A
Minimum Number of Simultaneous Minutiae of Mated Items	N/A	12	12	12	12
Selectivity	1	10/25	10/25	10/25	10/25
True Match Rate	99.9%	93%/100%	93%/100%	93%/100%	93%/100%
Non-Mated Search Records	50%	9,900	100	4,990	60
Background Repository	All Converted TP Records	All Converted LT Records	All Converted TP Records	All Converted Palm LT	All Converted KP Records

ATTACHMENT A.2
PROJECT DELIVERABLES
FOR
MBIS SOLUTION

ATTACHED TO STATEMENT OF WORK

ATTACHMENT A.3
PERFORMANCE REQUIREMENTS
FOR
MBIS SOLUTION

ATTACHED TO STATEMENT OF WORK

ATTACHMENT A.4
SYSTEM CONFIGURATION
FOR
MBIS SOLUTION

ATTACHED TO STATEMENT OF WORK

ATTACHMENT A.5
EXISTING SYSTEM REPORT
FOR
MBIS SOLUTION

INCORPORATED BY REFERENCE

EXHIBIT B
PRICING SCHEDULE
FOR
MBIS SOLUTION

1. GENERAL

This Exhibit B (Pricing Schedule) sets forth the pricing and payment terms for the Work to be provided by Contractor under the Agreement. The following Schedules are attached to and form a part of this Exhibit B:

- Schedule B.1 – Optional Work Schedule
- Schedule B.2 – Termination for Convenience Reimbursement
- Schedule B.3 – Additional Workstations

2. DELIVERABLES

There is no payment due to Contractor from County for Deliverables provided by Contractor during the System Implementation Phase of the Agreement.

3. SERVICE FEES

County will pay Contractor the Service Fees for System Maintenance, for periods commencing upon Final Acceptance, quarterly in arrears, in the amount equal to three (3) times the applicable Monthly Fees calculated based on the Annual Fees set forth below in this Section 3, as such amount may be appropriately adjusted for Service Credits or other adjustments allowed under the terms of the Agreement. Annual Fees, unless modified in accordance with Paragraph 4.2 (Change Notices) or Paragraph 4.3 (Amendments) of the Base Agreement, shall not increase above the amounts set forth below.

Table 41: Service Fees

SYSTEM OPERATION PHASE TERM	ANNUAL FEE	SUBTOTAL
Initial Term (Years 1 – 6 from Final Acceptance)	\$ 2,090,400	\$ 12,542,400
Extended Term (Years 7 – 10 from Final Acceptance)	\$ 1,970,400	\$ 7,881,600
TOTAL SERVICE FEES		\$20,424,000

4. OPTIONAL WORK

Any agreed upon Optional Work shall be provided by Contractor in accordance with *Paragraphs 5.4 (Optional Work) and 8.4 (Optional Work) of the Base Agreement*, following agreement by the parties on a not-to-exceed Maximum Fixed Price and the Scope of Work for such Optional Work. Any and all travel and living expenses, in order to be reimbursed by County, must be included in the Maximum Fixed Price quoted. If included in the Maximum Fixed Price, such travel and living expenses will be reimbursed only if reasonable, are quoted and approved in advance by County, are based on actual expenditures and do not exceed County's the then current travel expense reimbursement rates.

Any Professional Services provided by Contractor to County as part of Optional Work under the Agreement shall be calculated at the Fixed Hourly Rate of \$240.00 per hour. The Fixed Hourly Rate shall not increase during the term of the Agreement.

5. POOL DOLLARS

The Contract Sum includes an allocation of \$4,000,000 in Pool Dollars for acquisition of Optional Work, which is the maximum amount allocated for the term of the Agreement, unless modified by a duly authorized Amendment executed in accordance with Paragraph 4.3 (Amendments) of the Base Agreement. Pool Dollars may be used for acquiring Optional Work provided by Contractor pursuant to the applicable terms of the Agreement as specified in *Section 4 (Optional Work)* above by executing a Change Notice in accordance with *Paragraph 4.2 (Change Notices) or Paragraph 4.3 (Amendments) of the Base Agreement*, as applicable. Following acquisition of Optional Work using Pool Dollars, Schedule B.1 (Optional Work Schedule) shall be updated by County to reflect the Optional Work acquired and the remaining Pool Dollars balance.

6. CONTRACT SUM

Contract Sum shall be County's maximum obligation under the Agreement and shall include any and all amounts that may be paid by County to Contractor for System Maintenance and any Optional Work that County may request Contractor to provide during the term of the Agreement. The Contract Sum, unless modified in accordance with Paragraph 4.2 (Change Notices) or Paragraph 4.3 (Amendments) of the Base Agreement, including any and all sales tax amounts, if applicable, is Twenty Four Million Four Hundred Twenty Four Thousand Dollars (\$24,424,000) and includes the following components:

CONTRACT SUM COMPONENTS	TOTAL
Service Fees (10 years)	\$ 20,424,000
Pool Dollars (Agreement term)	\$ 4,000,000
CONTRACT SUM	\$ 24,424,000

SCHEDULE B.1
OPTIONAL WORK SCHEDULE
FOR
MBIS SOLUTION

SCHEDULE B.1

OPTIONAL WORK SCHEDULE

This Schedule B.1 shall be used by County to maintain listing of all Optional Work acquired by County under the Agreement using Pool Dollars and the remaining Pool Dollars following each such acquisition. This Schedule B.1 shall be included as part of a Change Notice or Amendment, as applicable, for each acquisition of Optional Work using Pool Dollars and shall be updated accordingly.

1. OPTIONAL WORK

In the event County elects to acquire any of the Optional Work specified below, such Optional Work shall be provided by Contractor to County at the applicable Maximum Fixed Price set forth in this Section 1 below.

ITEM NO.	DESCRIPTION / TYPE (APPLICATION MODIFICATIONS, PROFESSIONAL SERVICES, ADDITIONAL PRODUCTS, ETC.)	REQUEST DATE	DELIVERY DATE	COUNTY APPROVAL DATE	MAXIMUM FIXED PRICE
SUBTOTAL					\$ 0

2. POOL DOLLARS

EVENT (EFFECTIVE DATE, CHANGE NOTICE, AMENDMENT)	EVENT DATE	ADJUSTED AMOUNT ("+", "-")	REMAINING AMOUNT
Effective Date			\$ 4,000,000
Change Notice No. 1			

SCHEDULE B.2

**TERMINATION FOR CONVENIENCE REIMBURSEMENT
FOR
MBIS SOLUTION**

SCHEDULE B.2
TERMINATION FOR CONVENIENCE REIMBURSEMENT

This Schedule B.2 set forth the amounts County will be required to reimburse Contractor for the cost of the initial investment expended by Contractor in setting up the Solution and its environment in the event County, during the Initial Term of the Agreement, terminates this Agreement for convenience pursuant to Paragraph 21 (Termination for Convenience) of the Base Agreement.

Table 42: Termination for Convenience Reimbursement

PERIOD OF TERMINATION FOR CONVENIENCE	REIMBURSEMENT AMOUNT
Initial Term – Implementation Period	TBD based on documented actual costs incurred by Contractor at time of termination
Initial Term – Maintenance Period Year 1	\$ 6,814,799
Initial Term – Maintenance Period Year 2	\$ 5,508,531
Initial Term – Maintenance Period Year 3	\$ 4,089,371
Initial Term – Maintenance Period Year 4	\$ 2,636,874
Initial Term – Maintenance Period Year 5	\$ 1,247,034
Initial Term – Maintenance Period Year 6	\$ 461,053
Extended Term – Maintenance Period Year 7	\$ 0
Extended Term – Maintenance Period Year 8	\$ 0
Extended Term – Maintenance Period Year 9	\$ 0
Extended Term – Maintenance Period Year 10	\$ 0

The amount to be reimbursed by County to Contractor is for the hardware, software and services as defined in the Agreement, and will be based on the period during which the termination for convenience occurs and will assume that the termination occurs at the beginning of such period. Consequently, each applicable reimbursed amount will be offset by any and all Service Fees paid by County to Contractor during the period of such termination.

The reimbursement amounts specified above will not increase in the event (i) that County acquires any Optional Work under the Agreement by Change Notice or Amendment, as such shall be paid for by County under any such Change Notice or Amendment, or (ii) that Contractor implements a technology refresh or replacement in order to remain compliant with the System Requirements or otherwise the Agreement, as such are included in Contractor's System Maintenance obligations under the Agreement.

SCHEDULE B.3
ADDITIONAL WORKSTATIONS
FOR
MBIS SOLUTION

SCHEDULE B.3

ADDITIONAL WORKSTATIONS

This Schedule B.3 sets forth the pricing for any Additional Workstations that may be acquired by County from Contractor under the Agreement as Optional Work using Pool Dollars pursuant to an executed Change Notice or Amendment, as applicable. Unless specified otherwise in such Change Notice or Amendment, the Maximum Fixed Price amount for so acquired Additional Workstations shall be paid by County to Contractor in twelve (12) monthly installments without interest, as may further be specified in any such Change Notice or Amendment.

Any agreed upon payment for acquisition of Additional Workstations shall be due to Contractor following installation and deployment of such Additional Workstations at all facilities designated by County. Acquisition of Tenprint Suite, Latent Suite, Full Function Suite, Integra-ID Fast-ID Suite or NeoFace Reveal Suite Additional Workstations prior to the Final Acceptance shall be available at the applicable "Discount Purchase Price" set forth below. Applicable Annual Fees for System Maintenance may need to be amended as a result of any acquisition of Additional Workstations, as provided in the Agreement.

1. TENPRINT SUITE

Table 1: Tenprint Suite Pricing

Price Per Unit for complete complement of equipment including: - PC, Single 24-inch Monitor, Flatbed Scanner, UPS - Tenprint License and Software - Documentation, Installation and Shipping - Does not include training			
VOLUME	DISCOUNT PURCHASE PRICE PRIOR TO DEPLOYMENT	STANDARD PURCHASE PRICE YEAR 1 - 10	ANNUAL SERVICE FEE
1-5	\$16,340	\$28,700	\$3,500
6-10	\$16,340	\$25,400	\$3,500
11-15	\$16,340	\$22,200	\$3,500
16-25	\$16,340	\$19,200	\$3,500
26-50	\$16,340	\$17,200	\$3,500
50+	\$16,340	\$15,500	\$3,500

2. LATENT SUITE

Table 2: Latent Suite Pricing

Price Per Unit for complete complement of equipment including: - PC, Dual 24-inch Monitor, Flatbed Scanner, UPS - Latent License, Adobe Photoshop, and Software - Documentation, Installation and Shipping - Does not include training			
VOLUME	DISCOUNT PURCHASE PRICE PRIOR TO DEPLOYMENT	STANDARD PURCHASE PRICE YEAR 1 - 10	ANNUAL SERVICE FEE
1-5	\$18,525	\$37,400	\$4,400
6-10	\$18,525	\$31,120	\$4,400
11-15	\$18,525	\$26,550	\$4,400
16-25	\$18,525	\$22,500	\$4,400
26-50	\$18,525	\$19,500	\$4,400
50+	\$18,525	\$17,500	\$4,400

3. FULL FUNCTION (TENPRINT AND LATENT) SUITE

Table 3: Full Function (Tenprint and Latent) Pricing

Price Per Unit for complete complement of equipment including: - PC, Dual 24-inch Monitor, Flatbed Scanner, UPS - Tenprint and Latent License, Adobe Photoshop, and Software - Documentation, Installation and Shipping - Does not include training			
VOLUME	DISCOUNT PURCHASE PRICE PRIOR TO DEPLOYMENT	STANDARD PURCHASE PRICE YEAR 1 - 10	ANNUAL SERVICE FEE
1-5	\$23,608	\$49,200	\$5,900
6-10	\$23,608	\$39,900	\$5,900
11-15	\$23,608	\$34,000	\$5,900
16-25	\$23,608	\$29,800	\$5,900
26-50	\$23,608	\$24,850	\$5,900
50+	\$23,608	\$20,125	\$5,900

4. LATENT CAMERA

Table 4: Latent Camera Pricing

Price Per Unit for complete complement of equipment including: - Digital SLR - Camera Lens - Camera Stand and Illumination - Documentation, Installation and Shipping		
VOLUME	PURCHASE PRICE	ANNUAL SERVICE FEE
1-5	\$3,000	\$360
6-10	\$3,000	\$360
11-15	\$3,000	\$360
16-25	\$3,000	\$360
26-50	\$3,000	\$360
50+	\$3,000	\$360

5. PRINT SERVER

Table 5: Print Server Service Fee

Price Per Unit for complete complement of equipment including: - PC, Single 20-inch Monitor, UPS - Print Server License and Software - Installation and Shipping - Does not include training		
VOLUME	PURCHASE PRICE	ANNUAL SERVICE FEE
1-5	\$1,200	\$144
6-10	\$1,200	\$144
11-15	\$1,100	\$144
16-25	\$1,100	\$144
26-50	\$1,100	\$144
50+	\$1,100	\$144

6. FINGER PRINT CARD PRINTER

Table 6: Fingerprint Card Printer Pricing*

Price Per Unit for complete complement of equipment including: - IQS Certified Printer - Installation and Shipping		
VOLUME	PURCHASE PRICE	ANNUAL SERVICE FEE
1-5	\$2,000	\$240
6-10	\$2,000	\$240
11-15	\$2,000	\$240
16-25	\$2,000	\$240
26-50	\$2,000	\$240
50+	\$2,000	\$240

* Pricing may vary depending on market availability of certified FBI printers.

7. INTEGRA-ID FAST ID SUITE

Table 7: Integra-ID Fast ID Service Fee

Price Per Unit for complete complement of equipment including: - PC, Single 20-inch Monitor, Single Finger Scanner, UPS - Fast ID License and Software - Documentation, Installation and Shipping - Does not include training			
VOLUME	PURCHASE PRICE PRIOR TO DEPLOYMENT	PURCHASE PRICE YEAR 1 - 10	ANNUAL SERVICE FEE
1-5	\$4,028	\$4,600	\$552
6-10	\$4,028	\$4,600	\$552
11-15	\$4,028	\$4,520	\$552
16-25	\$4,028	\$4,520	\$552
26-50	\$4,028	\$4,475	\$552
50+	\$4,028	\$4,475	\$552

8. NEOFACE REVEAL SUITE

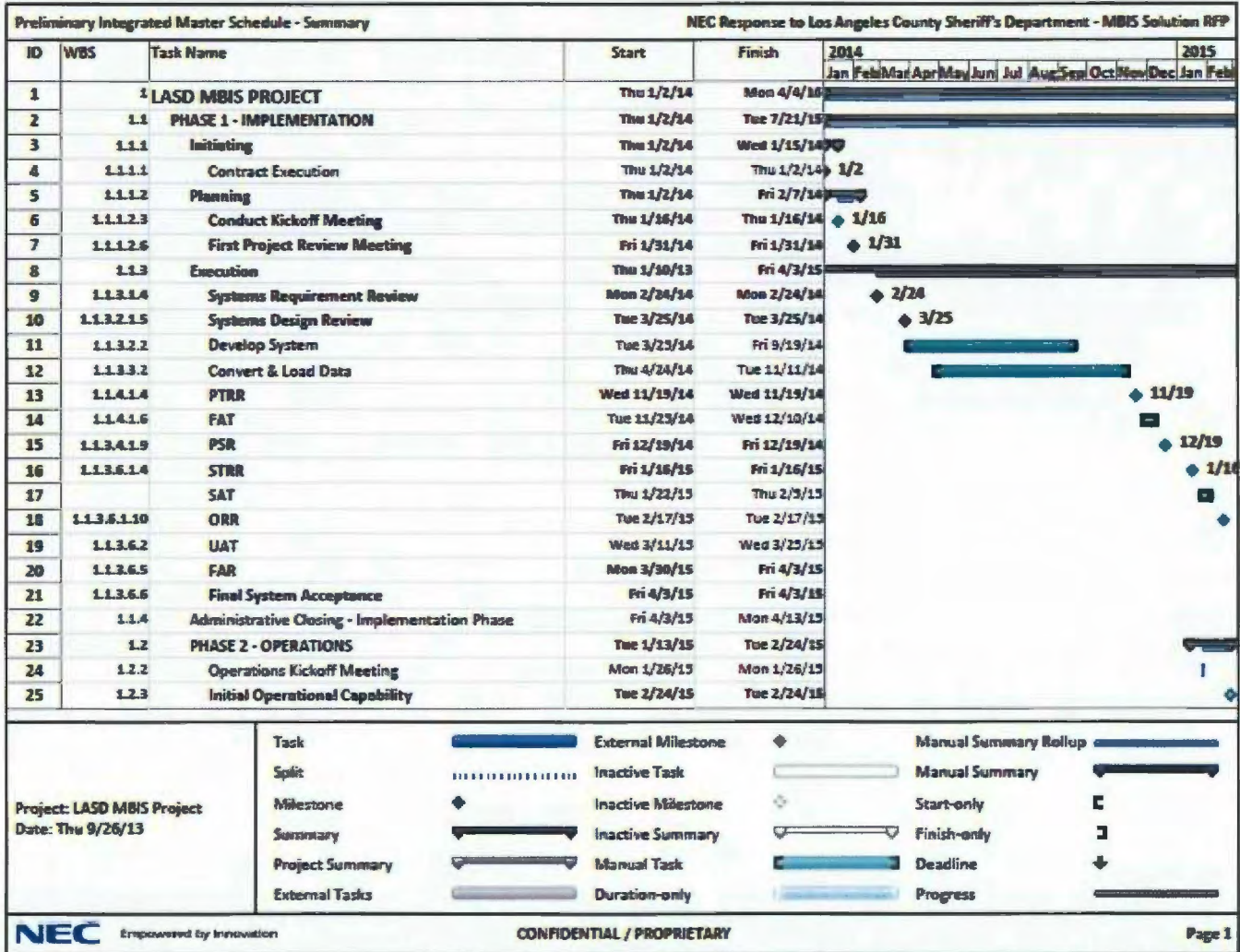
Table 8: NeoFace Reveal Service Fee

Price Per Unit for complete complement of equipment including: - 27-inch Touch All-in-one, UPS - Reveal License and Software - Documentation, Installation and Shipping - Does not include training			
VOLUME	DISCOUNT PURCHASE PRICE PRIOR TO DEPLOYMENT	STANDARD PURCHASE PRICE YEAR 1 - 10	ANNUAL SERVICE FEE
1-5	\$28,800	\$37,100	\$4,452
6-10	\$28,800	\$36,500	\$4,452
11-15	\$28,800	\$35,000	\$4,452
16-25	\$28,800	\$35,000	\$4,452
26-50	\$28,800	\$32,000	\$4,452
50+	\$28,800	\$30,250	\$4,452

EXHIBIT C
PROJECT SCHEDULE
FOR
MBIS SOLUTION

(PRELIMINARY)

EXHIBIT C PROJECT SCHEDULE



NEC

Empowered by Innovation

CONFIDENTIAL / PROPRIETARY

Page 1

EXHIBIT D
SERVICE LEVEL REQUIREMENTS
FOR
MBIS SOLUTION

EXHIBIT D

SERVICE LEVEL REQUIREMENTS

Contractor and the Solution shall meet the Service Level Requirements set forth in this Exhibit D.

PERFORMANCE REQUIREMENTS

The Service Level Plan, to be provided by Contractor in accordance with the SOW, which meet all Service Level Requirements, including those set forth in Section 3 – System Operation of the SOW.

SECTION 1 STORAGE CAPACITY REQUIREMENTS

Storage capacities are relevant to the following areas of the MBIS System architecture, including:

- ANSI/NIST Archive
- The templates/features loaded in the matchers

The following under this Section 1 – *STORAGE CAPACITY REQUIREMENTS* delineate these requirements and will refer to the tables provided below.

SECTION 1.1 ANNUAL SYSTEM MATRIX

RECORD TYPE	2009	2010	2011	2012	GROWTH RATE
Registered MAIN Numbers	3,896,801	4,021,159	4,141,491	4,234,079	2%
Records in NIST Archive	3,480,469	3,859,862	4,223,479	4,588,630	2%
Tenprint Searches	408,685	451,997	369,497	357,941	2%

SECTION 1.2 CURRENT LACRIS RECORD COUNTS

LACRIS RECORD TYPE	OCTOBER 2012	JANUARY 2013
Tenprints	11,740,616	11,885,223
MAIN Subjects	4,336,089	4,372,098
Palm Prints	N/A	2,257,182
Unsolved Latent	233,882	240,025
Unsolved Palm Latent	92,137	95,580

The MBIS will be designed to accommodate an ANSI/NIST Archive of all input and output transactions through the term of the Agreement. The addition of response TOTs will make the capacity requirements larger than the storage of input transactions only. Most response transactions generated by the MBIS are smaller than the corresponding input transactions. The Contractor will have to perform the appropriate design analysis to determine the design requirements in terms of terabytes as a function of transaction type using the data specified in this document.

At the initial operating point of the MBIS, all existing records will have been loaded into the MBIS, including into the ANSI/NIST Archive, the matchers, any other repositories and the master index.

SECTION 2 SYSTEM PERFORMANCE REQUIREMENTS

The MBIS must meet the Performance Requirements (throughput and Response Time) as specified in this Section 2 – *SYSTEM PERFORMANCE REQUIREMENTS*. The MBIS throughput rates will grow over the life of the System. The following table projects the growth for the Existing Agreement.

SECTION 2.1 ANNUAL LACRIS TRANSACTION COUNTS

TRANSACTION TYPE	2010	2011	2012	GROWTH RATE
CRM	373,436	350,924	327,197	2%
CUS	0	0	0	2%
REG	5,085	6,427	8,840	2%
SUP	0	0	0	0
COR	0	0	0	0
IDN	41,137	23,444	12,646	2%
IDN2	916	0	0	2%
IDN4	306,073	392,822	339,629	10%
APP	1	1	0	2%
Latent	44,289	54,179	58,737	2%
Palm Latent	18,023	27,803	29,023	2%
TLI	<u>382,409</u>	<u>363,730</u>	<u>345,118</u>	2%
TOTAL	1,171,369	1,219,330	1,121,190	

Legend:

- CRM – criminal booking
- CUS – custody TOT, this is for the inmate realignment. State prisoners being moved to counties
- REG – registrant TOT
- SUP – supplemental
- COR – coroner, deceased
- IDN – identification transaction, state transaction, full roll
- IDN2 – county ID transaction, two index fingers
- IDN4 – county ID transaction, flats (four finger and thumbs)
- APP – applicant (not retained in our AFIS, passed through to DOJ)
- Latent – latent search
- Palm Latent – palm latent
- TLI – tenprint to latent ID.

SECTION 3 RESPONSE TIME REQUIREMENTS

The Response Time for MBIS transactions is a function of the transaction type (identification, forensic, and tactical (Mobile ID)). The Response Times do not include any human interaction times.

The table below provides the Response Times per class of transaction, while the Response Time Requirements table defines the requirements for providing these Response Times.

SECTION 3.1 RESPONSE TIMES PER TRANSACTION TYPE

TRANSACTION CLASS TYPES	RESPONSE REQUIREMENTS UNDER PEAK LOAD
Criminal TP-TP	1 minute
TP-LT	1 minute
LT-TP	1 minute
Palm LT-KP	10 minutes
Criminal KP-LT	5 minutes
Mobile ID TP-TP	30 seconds

SECTION 4 ACCURACY REQUIREMENTS

The matcher accuracy will vary as a function of the class of service (identification, forensic and tactical (Mobile ID)) and the quality of the input images. Identification service accuracy requirements are typically higher than those for forensic services, as the input images are typically of better quality for Live-Scan enrollments than for latent lifts.

Accuracy terms-of-art have been undergoing an evolutionary change for the past few years. While reliability, true accept rate, false reject rate and other terms are often used for access control systems and other biometric modalities (such as facial recognition), a consensus has developed in the international standards community around the terms *true match rate* and *failure to match rate* when discussing friction ridge matching on a large scale.

For this project accuracy will include three (3) accuracy terms:

- *True Match Rate* – the probability that a true match will be found when it is in the background reference file (also known as a repository). This term replaces older terminology such as matcher reliability or true accept rate.
- *Failure to Match Rate* – the probability that a search will not return a true match when the true match is in the reference file. The failure to match rate is 100 percent minus the true match rate. While not explicitly stated in the requirements, it will be calculated during testing and reported.
- *Selectivity* – the number of candidates that will be examined to determine the true match rate. While the system administrators will be able to selectively change the length of candidate lists by transaction class, and by threshold scores, during testing, System accuracy will be measured using the selectivity numbers shown in the table that follows.

SECTION 4.1 ACCURACY RATES BY TRANSACTION TYPE

TRANSACTION TYPES	SELECTIVITY	TRUE MATCH RATE
TP-TP	1	99.9%
Mobile ID TP-TP (with fewer than 10 prints)	8	99.9%
TP-LT	10/25	93%/100%
Criminal KP-LT	10/25	93%/100%
LT-TP	10/25	93%/100%
Palm LT-KP	10/25	93%/100%

SECTION 5 ACCURACY VERIFICATION REQUIREMENTS AND MEASURES

SECTION 5.1 LIGHTS OUT ACCURACY VERIFICATION CONDITIONS

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Search Records	10,000	10,000	200	5,000	100
Mated Records	50%	100	100	10	40
NFIQ Average of Mated TPs	3.1 or Better	3.1 or Better	3.1 or Better	N/A	N/A
Minimum Number of Simultaneous Minutiae of Mated Items	N/A	16	16	16	16
Selectivity ¹	1	10/25	10/25	10/25	10/25
True Match Rate ²	99.8%	45%/60%	45%/60%	45%/60%	45%/60%
Non-Mated Search Records	50%	9,900	100	4,990	60
Background Repository	All Converted TP Records	All Converted LT Records	All Converted TP Records	All Converted Palm LT Records	All Converted KP Records

1. Selectivity is a measure of allowed candidate list length.

2. Assumes a true match is in the searched file.

SECTION 5.2**BEST PRACTICES VERIFICATION CONDITIONS**

ELEMENT	TP-TP	TP-LT	LT-TP	KP-PLT	PLT-KP
Search Records	10,000	10,000	200	5,000	100
Mated Records	50%	100	100	10	40
NFIQ Average of Mated TPs	1	1	1	N/A	N/A
Minimum Number of Simultaneous Minutiae of Mated Items	N/A	12	12	12	12
Selectivity	1	10/25	10/25	10/25	10/25
True Match Rate	99.9%	93%/100%	93%/100%	93%/100%	93%/100%
Non-Mated Search Records	50%	9,900	100	4,990	60
Background Repository	All Converted TP Records	All Converted LT Records	All Converted TP Records	All Converted Palm LT Records	All Converted KP Records

SECTION 6 SERVICE AVAILABILITY AND RESTORATION REQUIREMENTS

Given that the MBIS will operate under a COOP to include a Disaster Recovery Site (COOP Site), it is anticipated that MBIS Services will have a very high level of continuous availability.

The Service Availability of all MBIS Services must be at a minimum 99.8 percent (99.8%) per month without any allowance beyond 99.8 percent (99.8%) for Scheduled Downtime or switchover from the Primary Site to the COOP Site (or vice versa). Service Availability of 99.8 percent (99.8%) leaves a little less than 90 minutes a month for Service outages at the MBIS level. Contractor may roll Scheduled Downtime between the Primary Site and COOP Site to preclude as many MBIS Service outages as possible. The reasons for the COOP Site include:

- To provide for fast recovery for failed equipment and localized power outages at the Primary Site with 99.8 (99.8%) percent Service Availability as a requirement. This includes provision of any and all Necessary power conditioning and alternative power sourcing to maintain the Service Availability requirement.
- To provide the basis for recovery of services in the event of a catastrophic failure at the Primary Site (fire, explosion, radioactive contaminations, etc.).

SECTION 7 SYSTEM MAINTENANCE REQUIREMENTS

Contractor shall perform Preventive Maintenance and Corrective Maintenance as a part of the monthly Service Fee and at no additional cost to County.

SECTION 7.1 PREVENTIVE MAINTENANCE

Unless agreed to otherwise in advance by County and Contractor, Contractor shall provide all Preventive Maintenance Services during Scheduled Downtime, during late evening hours or early morning hours in order to avoid times when users need to use the System, as agreed to by County.

Contractor will perform a documented Preventive Maintenance procedure for all equipment and software they provide. Contractor shall periodically dispatch maintenance personnel to clean, inspect and adjust the equipment and replace defective or worn parts thereof at the manufacturer's recommended frequency in order to keep the equipment in good operating condition. Contractor shall carry out periodic maintenance tasks on all electronic components they provide to ensure they are operating at maximum capability. Such maintenance shall be scheduled to be performed, at a minimum, once a month during hours agreed to by County.

SECTION 7.2 CORRECTIVE MAINTENANCE

Contractor shall provide corrective maintenance for any Deficiency in Contractor provided equipment or software that, when used as delivered, fails to perform in accordance with the Specifications specified in the Agreement, including System Requirements. The period for the provision of corrective Maintenance coverage for all hardware and software shall be defined as 24/7.

Contractor shall maintain an electronic report log that indicates the problem report number, problem description, the time that the problem call was received, the priority assigned, all actions taken and the time that the problem was corrected. The problem report log shall be maintained in a database that is remotely accessible by County personnel.

Contractor shall offer one central point of contact for support of hardware and software. Contractor support personnel shall address all problems reported by County's Help Desk staff. Contractor's support personnel shall acknowledge problems reported via telephone or by e-mail within one (1) hour and respond according to the protocols listed below.

SECTION 7.3 PROTOCOLS

County shall assign the Priority Level to each Deficiency reported by County to Contractor's Customer Support. Contractor shall assign Priority Levels to Deficiencies discovered by its own problem monitoring system. Following report of a Deficiency from County, Contractor shall respond back to County within the prescribed "Response Timeframe" specified below and resolve each such Deficiency within the specified "Resolution Time". Resolution Time for correction of Deficiencies shall start tolling when County first notifies Contractor of a Deficiency by telephone or otherwise as specified herein, including Contractor's Customer Support, and shall end when County determines that the Deficiency has been resolved.

Problems that require an immediate response (Priority Level 1) are System or component failures that prevent subjects from being enrolled, images from being searched or responses from being delivered. This includes all equipment supplied by Contractor associated with the System, including Remote Site printers, scanners and other required peripherals that would prevent users from accomplishing their work.

Contractor may attempt to correct the problem by phone or remote access. If Contractor is unable to correct the problem in this manner, Contractor must begin on-site repair within four (4) hours of the time Contractor was initially notified, depending on the availability of the site where the equipment resides. All situations that prevent the initiation of on-site repair within such four (4) hours will be documented in Contractor's electronic report log and reported to County's Help Desk.

Contractor must ensure that the equipment will be repaired within eight (8) consecutive hours. If a device is out of service for eight (8) consecutive hours from the time Contractor was notified, Contractor shall, by the end of the eighth hour, replace the defective equipment with an operable device until the defective item has been fully repaired. The eight (8) hour clock begins from the time of personal notification to Contractor.

All other Major Deficiencies (Priority Level 2) will be corrected within two (2) Business Days from the time the problem was reported.

Contractor shall inform County within 1 hour of any service interruptions and then notify the County within eight (8) hours of any hardware or software problems that Contractor has identified and resolved.

EXHIBIT E

**ADMINISTRATION OF AGREEMENT
FOR
MBIS SOLUTION**

EXHIBIT E
ADMINISTRATION OF AGREEMENT

SECTION 1 – COUNTY KEY PERSONNEL

COUNTY’S PROJECT DIRECTOR:

NAME: Joshua W. Thai
TITLE: Lieutenant
ADDRESS: 12440 E. Imperial Highway, # 400
Norwalk, CA 90650
TELEPHONE: (562) 345-4319
FACSIMILE: (323) 415-2905
E-MAIL ADDRESS: JWTHAI@LASD.ORG

COUNTY’S PROJECT MANAGER:

NAME: Michael J. Kampen
TITLE: Sergeant
ADDRESS: 12440 E. Imperial Highway, # 400
Norwalk, CA 90650
TELEPHONE: (562) 345-4340
FACSIMILE: (323) 415-1355
E-MAIL ADDRESS: MIKAMPEN@LASD.ORG

DIRECTOR:

NAME: Jim McDonnell
TITLE: Sheriff
ADDRESS: 4700 Ramona Blvd.
Monterey Park, CA 91754
TELEPHONE: (323) 526-5000
FACSIMILE: (323) 415-1060
E-MAIL ADDRESS: JMCDONNE@LASD.ORG

SECTION 2 – CONTRACTOR KEY PERSONNEL

CONTRACTOR'S PROJECT DIRECTOR:

NAME: Roger Konecny
TITLE: Project Director
ADDRESS: 10850 Gold Center Drive, Suite 200
Rancho Cordova, CA 95670
TELEPHONE: (916) 463-7033
FACSIMILE: (916) 463-7041
E-MAIL ADDRESS: Roger.konecny@necam.com

CONTRACTOR'S PROJECT MANAGER:

NAME: Sam Gonzalez
TITLE: Project Manager
ADDRESS: 10850 Gold Center Drive, Suite 200
Rancho Cordova, CA 95670
TELEPHONE: (714) 335-4152
FACSIMILE: (916) 463-7041
E-MAIL ADDRESS: Samuel.Gonzalez@necam.com

CONTRACTOR'S PROJECT EXECUTIVE:

NAME: Raffie Beroukhim
TITLE: Vice President
ADDRESS: 10850 Gold Center Drive, Suite 200
Rancho Cordova, CA 95670
TELEPHONE: (916) 607-5842
FACSIMILE: (916) 463-7041
E-MAIL ADDRESS: Raffie.Beroukhim@necam.com

EXHIBIT F
CONFIDENTIALITY AND ASSIGNMENT AGREEMENT
FOR
MBIS SOLUTION

EXHIBIT F

CONFIDENTIALITY AND ASSIGNMENT AGREEMENT

CONTRACTOR: NEC Corporation of America

1. GENERAL INFORMATION

The organization identified above ("Contractor") is under contract ("Contract") to provide Work (as such term is defined in the Contract) to the County of Los Angeles ("County"). County requires each employee, agent, consultant, outsourced vendor and independent contractor of this Contractor performing Work under such Contract to understand his/her obligations with respect to the personal, proprietary and other confidential material, data or information, with which he/she will be in contact. Contractor, by executing this Confidentiality and Assignment Agreement (also "Agreement"), represents that it shall ensure each such staff member's compliance with the obligations regarding such data and information, as set forth in the Base Agreement, including this Exhibit F.

2. CONTRACTOR ACKNOWLEDGMENT

Contractor understands and agrees that all of Contractor's, or any subcontractor's, staff that will provide Work pursuant to the above-referenced Contract are Contractor's, or any subcontractor's, sole responsibility. Contractor understands and agrees that its, or any subcontractor's, staff must rely exclusively upon Contractor, or any subcontractor, for payment of salary and any and all other benefits payable by virtue of such staff's performance of Work under this Agreement.

Contractor understands and agrees that its, or any subcontractor's, employees are not employees of County for any purpose whatsoever and that such staff do not have and will not acquire any rights or benefits of any kind from County by virtue of performance of Work under the above-referenced Contract. Contractor understands and agrees that its, or any subcontractor's, staff do not have and will not acquire any rights or benefits from County pursuant to any agreement between any person or entity and County.

3. CONFIDENTIALITY

Contractor, any subcontractor, and their staff, by virtue of performing Work under the above-referenced Contract, may come in contact with (i) County's Confidential Information (as such term is defined in the Base Agreement to the Contract), (ii) data and information, which County has an obligation to keep confidential by applicable law or otherwise, and (iii) proprietary information belonging to other organizations doing business with County (collectively for the purpose of this Exhibit F "Confidential Information"). By signing this Agreement, Contractor agrees that, by virtue of involvement in the Work under the Contract, it, any subcontractor, and their staff shall protect the confidentiality of all such Confidential Information pursuant to the terms of Paragraph 18 (Confidentiality and Security) of the Base Agreement and as specified below.

Contractor agrees, on behalf of itself, its subcontractors and all staff, (i) to protect from loss and hold in confidence any and all Confidential Information; (ii) not to directly or indirectly reveal,

report, publish, transfer, reproduce to, or for the benefit of, any unauthorized person or otherwise disclose any of County's Confidential Information obtained while performing Work under the above-referenced Contract; and (iii) to utilize the Confidential Information solely for the limited purpose of providing Work pursuant to the Contract. Contractor's, or any subcontractor's, staff shall forward all requests for disclosure or copying of any such information in their possession or care to County's Project Manager identified under the Contract.

Contractor agrees to report to County's Project Manager under the Contract any and all violations of this Agreement, including unauthorized disclosures or copying of Confidential Information, whether accidental or intentional, and whether by Contractor's, or any subcontractor's, staff and/or by any other person, of which such staff become aware. Contractor agrees and shall ensure that its, or any subcontractor's, staff return possession of all County's Confidential Information to County's Project Manager under the Contract upon completion of the above-referenced Contract or termination of employment with Contractor, or any subcontractor, whichever occurs first.

4. ASSIGNMENT OF PROPRIETARY RIGHTS

All County Materials, excluding the Work Product and System Software provided by Contractor and related Documentation (as defined in Paragraph 16 (Proprietary Conditions) of the Base Agreement), shall belong exclusively to County whether or not fixed in a tangible medium of expression. Without limiting the foregoing, to the maximum extent permitted under applicable law, all County Materials shall be deemed to be "works made for hire" under the United States Copyright Act, and County shall be deemed to be the author thereof.

If and to the extent any County Materials are determined not to constitute "works made for hire", or if any rights in the County Materials do not accrue to County as a work made for hire, Contractor agrees to ensure that all right, title and interest in such County Materials, including but not limited to all copyrights, patents, trade secret rights and other proprietary rights in or relating to the County Materials, are irrevocably assigned and transferred to County to the maximum extent permitted by law. Without limiting the foregoing, Contractor agrees to ensure that (i) all economic rights to the County Materials, including the exclusive and unrestricted right to reproduce, manufacture, use, adapt, modify, publish, distribute, sublicense, publicly perform and communicate, translate, lease, import, export, transfer, convey and otherwise exploit the County Materials, are assigned and transferred to County; (ii) County is entitled to any and all modifications, uses, publications and other exploitation of the County Materials without consequences; and (iii) County obtains United States or any foreign letters patent, copyright registrations and other proprietary rights covering inventions and original works of authorship in the County Materials.

Furthermore, Contractor agrees to execute all necessary documents and to perform all other acts in order to assign all of Contractor's right, title and interest in the County Materials in accordance with the Base Agreement.

SIGNED _____

DATE _____

PRINTED Raffie Beroukhim

TITLE VP Biometric Solutions Division

EXHIBIT G
CONTRACTOR'S EEO CERTIFICATION
FOR
MBIS SOLUTION

EXHIBIT G
CONTRACTOR'S EEO CERTIFICATION

NEC Corporation of America

Company Name

6535 N. State Highway 161, Irving, TX 75039

Address

FEIN #20-0665337

Internal Revenue Service Employer Identification Number

GENERAL

In accordance with provisions of the County Code of the County of Los Angeles, Contractor certifies and agrees that all persons employed by such firm, its affiliates, subsidiaries and holding companies are and will be treated equally by the firm without regard to or because of race, religion, ancestry, national origin, age or sex and in compliance with all anti-discrimination laws of the United States of America and the State of California.

CERTIFICATION

	<u>YES</u>	<u>NO</u>
1. Contractor has a written policy statement prohibiting discrimination in all phases of employment.	()	(x)
2. Contractor periodically conducts a self-analysis or utilization analysis of its work force.	()	(x)
3. Contractor has a system for determining if its employment practices are discriminatory against protected groups.	()	(x)
4. When problem areas are identified in employment practices, Contractor has a system for taking reasonable corrective action to include establishment of goal and/or timetables.	()	(x)

Signature

Date

Raffie Beroukhim, VP Biometric Solutions Division

Name and Title of Signer (please print)

EXHIBIT H
JURY SERVICE ORDINANCE
FOR
MBIS SOLUTION

Title 2 ADMINISTRATION
Chapter 2.203.010 through 2.203.090
CONTRACTOR EMPLOYEE JURY SERVICE

2.203.010 Findings.

The board of supervisors makes the following findings. The county of Los Angeles allows its permanent, full-time employees unlimited jury service at their regular pay. Unfortunately, many businesses do not offer or are reducing or even eliminating compensation to employees who serve on juries. This creates a potential financial hardship for employees who do not receive their pay when called to jury service, and those employees often seek to be excused from having to serve. Although changes in the court rules make it more difficult to excuse a potential juror on grounds of financial hardship, potential jurors continue to be excused on this basis, especially from longer trials. This reduces the number of potential jurors and increases the burden on those employers, such as the county of Los Angeles, who pay their permanent, full-time employees while on juror duty. For these reasons, the county of Los Angeles has determined that it is appropriate to require that the businesses with which the county contracts possess reasonable jury service policies. (Ord. 2002-0015 § 1 (part), 2002)

2.203.020 Definitions.

The following definitions shall be applicable to this chapter:

- A. "Contractor" means a person, partnership, corporation or other entity which has a contract with the county or a subcontract with a county contractor and has received or will receive an aggregate sum of \$50,000 or more in any 12-month period under one or more such contracts or subcontracts.
- B. "Employee" means any California resident who is a full-time employee of a contractor under the laws of California.
- C. "Contract" means any agreement to provide goods to, or perform services for or on behalf of, the county but does not include:
 - 1. A contract where the board finds that special circumstances exist that justify a waiver of the requirements of this chapter; or
 - 2. A contract where federal or state law or a condition of a federal or state program mandates the use of a particular contractor; or
 - 3. A purchase made through a state or federal contract; or
 - 4. A monopoly purchase that is exclusive and proprietary to a specific manufacturer, distributor, or reseller, and must match and inter-member with existing supplies, equipment or systems maintained by the county pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section P-3700 or a successor provision; or
 - 5. A revolving fund (petty cash) purchase pursuant to the Los Angeles County Fiscal Manual, Section 4.4.0 or a successor provision; or
 - 6. A purchase card purchase pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section P-2810 or a successor provision; or
 - 7. A non-agreement purchase with a value of less than \$5,000 pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section A-0300 or a successor provision; or
 - 8. A bona fide emergency purchase pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section PP-1100 or a successor provision.

Title 2 ADMINISTRATION
Chapter 2.203.010 through 2.203.090
CONTRACTOR EMPLOYEE JURY SERVICE

Page 2 of 3

- D. "Full time" means 40 hours or more worked per week, or a lesser number of hours if:
1. The lesser number is a recognized industry standard as determined by the chief administrative officer, or
 2. The contractor has a long-standing practice that defines the lesser number of hours as full time.
- E. "County" means the county of Los Angeles or any public entities for which the board of supervisors is the governing body. (Ord. 2002-0040 § 1, 2002: Ord. 2002-0015 § 1 (part), 2002)

2.203.030 Applicability.

This chapter shall apply to contractors who enter into contracts that commence after July 11, 2002. This chapter shall also apply to contractors with existing contracts which are extended into option years that commence after July 11, 2002. Contracts that commence after May 28, 2002, but before July 11, 2002, shall be subject to the provisions of this chapter only if the solicitations for such contracts stated that the chapter would be applicable. (Ord. 2002-0040 § 2, 2002: Ord. 2002-0015 § 1 (part), 2002)

2.203.040 Contractor Jury Service Policy.

A contractor shall have and adhere to a written policy that provides that its employees shall receive from the contractor, on an annual basis, no less than five days of regular pay for actual jury service. The policy may provide that employees deposit any fees received for such jury service with the contractor or that the contractor deduct from the employees' regular pay the fees received for jury service. (Ord. 2002-0015 § 1 (part), 2002)

2.203.050 Other Provisions.

- A. Administration. The chief administrative officer shall be responsible for the administration of this chapter. The chief administrative officer may, with the advice of county counsel, issue interpretations of the provisions of this chapter and shall issue written instructions on the implementation and ongoing administration of this chapter. Such instructions may provide for the delegation of functions to other county departments.
- B. Compliance Certification. At the time of seeking a contract, a contractor shall certify to the county that it has and adheres to a policy consistent with this chapter or will have and adhere to such a policy prior to award of the contract. (Ord. 2002-0015 § 1 (part), 2002)

2.203.060 Enforcement and Remedies.

For a contractor's violation of any provision of this chapter, the county department head responsible for administering the contract may do one or more of the following:

1. Recommend to the board of supervisors the termination of the contract; and/or,
2. Pursuant to chapter 2.202, seek the debarment of the contractor. (Ord. 2002-0015 § 1 (part), 2002)

Title 2 ADMINISTRATION
Chapter 2.203.010 through 2.203.090
CONTRACTOR EMPLOYEE JURY SERVICE

Page 3 of 3

2.203.070. Exceptions.

- A. Other Laws. This chapter shall not be interpreted or applied to any contractor or to any employee in a manner inconsistent with the laws of the United States or California.
- B. Collective Bargaining Agreements. This chapter shall be superseded by a collective bargaining agreement that expressly so provides.
- C. Small Business. This chapter shall not be applied to any contractor that meets all of the following:
 - 1. Has ten or fewer employees during the contract period; and,
 - 2. Has annual gross revenues in the preceding twelve months which, if added to the annual amount of the contract awarded, are less than \$500,000; and,
 - 3. Is not an affiliate or subsidiary of a business dominant in its field of operation.

"Dominant in its field of operation" means having more than ten employees and annual gross revenues in the preceding twelve months which, if added to the annual amount of the contract awarded, exceed \$500,000.

"Affiliate or subsidiary of a business dominant in its field of operation" means a business which is at least 20 percent owned by a business dominant in its field of operation, or by partners, officers, directors, majority stockholders, or their equivalent, of a business dominant in that field of operation. (Ord. 2002-0015 § 1 (part), 2002)

2.203.090. Severability.

If any provision of this chapter is found invalid by a court of competent jurisdiction, the remaining provisions shall remain in full force and effect. (Ord. 2002-0015 § 1 (part), 2002)

EXHIBIT I

**SAFELY SURRENDERED BABY LAW
FOR
MBIS SOLUTION**

Safely Surrendered



No shame. No blame. No names.

In Los Angeles County: 1-877-BABY SAFE • 1-877-222-9723

www.babysafeLA.org



Safely Surrendered Baby Law

What is the Safely Surrendered Baby Law?

California's Safely Surrendered Baby Law allows parents or other persons, with lawful custody, which means anyone to whom the parent has given permission to confidentially surrender a baby. As long as the baby is three days (72 hours) of age or younger and has not been abused or neglected, the baby may be surrendered without fear of arrest or prosecution.

In Los Angeles County: 1 877 BABY SAFE 1 877 222 9723

www.babysafela.org

How does it work?

A distressed parent who is unable or unwilling to care for a baby can legally, confidentially, and safely surrender a baby within three days (72 hours) of birth. The baby must be handed to an employee at a hospital or fire station in Los Angeles County. As long as the baby shows no sign of abuse or neglect, no name or other information is required. In case the parent changes his or her mind at a later date and wants the baby back, staff will use bracelets to help connect them to each other. One bracelet will be placed on the baby, and a matching bracelet will be given to the parent or other surrendering adult.

What if a parent wants the baby back?

Parents who change their minds can begin the process of reclaiming their baby within 14 days. These parents should call the Los Angeles County Department of Children and Family Services at 1-800-540-4000.

Can only a parent bring in the baby?

No. While in most cases a parent will bring in the baby, the Law allows other people to bring in the baby if they have lawful custody.

Does the parent or surrendering adult have to call before bringing in the baby?

No. A parent or surrendering adult can bring in a baby anytime, 24 hours a day, 7 days a week, as long as the parent or surrendering adult surrenders the baby to someone who works at the hospital or fire station.

Does the parent or surrendering adult have to tell anything to the people taking the baby?

No. However, hospital or fire station personnel will ask the surrendering party to fill out a questionnaire designed to gather important medical history information, which is very useful in caring for the baby. The questionnaire includes a stamped return envelope and can be sent in at a later time.

What happens to the baby?

The baby will be examined and given medical treatment. Upon release from the hospital, social workers immediately place the baby in a safe and loving home and begin the adoption process.

What happens to the parent or surrendering adult?

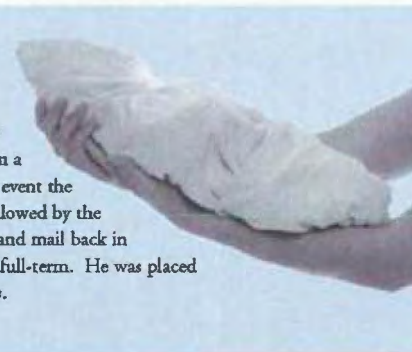
Once the parent or surrendering adult surrenders the baby to hospital or fire station personnel, they may leave at any time.

Why is California doing this?

The purpose of the Safely Surrendered Baby Law is to protect babies from being abandoned, hurt or killed by their parents. You may have heard tragic stories of babies left in dumpsters or public bathrooms. Their parents may have been under severe emotional distress. The mothers may have hidden their pregnancies, fearful of what would happen if their families found out. Because they were afraid and had no one or nowhere to turn for help, they abandoned their babies. Abandoning a baby is illegal and places the baby in extreme danger. Too often, it results in the baby's death. The Safely Surrendered Baby Law prevents this tragedy from ever happening again in California.

A baby's story

Early in the morning on April 9, 2005, a healthy baby boy was safely surrendered to nurses at Harbor-UCLA Medical Center. The woman who brought the baby to the hospital identified herself as the baby's aunt and stated the baby's mother had asked her to bring the baby to the hospital on her behalf. The aunt was given a bracelet with a number matching the anklet placed on the baby; this would provide some identification in the event the mother changed her mind about surrendering the baby and wished to reclaim the baby in the 14-day period allowed by the Law. The aunt was also provided with a medical questionnaire and said she would have the mother complete and mail back in the stamped return envelope provided. The baby was examined by medical staff and pronounced healthy and full-term. He was placed with a loving family that had been approved to adopt him by the Department of Children and Family Services.



Ley de Entrega de Bebés *Sin Peligro*



*Los recién nacidos pueden ser entregados en forma segura al personal
de cualquier hospital o cuartel de bomberos del Condado de Los Ángeles*

Sin pena. Sin culpa. Sin nombres.

En el Condado de Los Ángeles: 1-877-BABY SAFE • 1-877-222-9723

www.babysafela.org



Ley de Entrega de Bebés Sin Peligro

¿Qué es la Ley de Entrega de Bebés sin Peligro?

La Ley de Entrega de Bebés sin Peligro de California permite la entrega confidencial de un recién nacido por parte de sus padres u otras personas con custodia legal, es decir cualquier persona a quien los padres le hayan dado permiso. Siempre que el bebé tenga tres días (72 horas) de vida o menos, y no haya sufrido abuso ni negligencia, pueden entregar al recién nacido sin temor de ser arrestados o procesados.

Cada recién nacido se merece la oportunidad de tener una vida saludable. Si alguien que usted conoce está pensando en abandonar a un recién nacido, infórmele que tiene otras opciones. Hasta tres días (72 horas) después del nacimiento, se puede entregar un recién nacido al personal de cualquier hospital o cuartel de bomberos del condado de Los Angeles.

¿Cómo funciona?

El padre/madre con dificultades que no pueda o no quiera cuidar de su recién nacido puede entregarlo en forma legal, confidencial y segura dentro de los tres días (72 horas) del nacimiento. El bebé debe ser entregado a un empleado de cualquier hospital o cuartel de bomberos del Condado de Los Angeles. Siempre que el bebé no presente signos de abuso o negligencia, no será necesario suministrar nombres ni información alguna. Si el padre/madre cambia de opinión posteriormente y desea recuperar a su bebé, los trabajadores utilizarán brazaletes para poder vincularlos. El bebé llevará un brazaletes y el padre/madre o el adulto que lo entregue recibirá un brazaletes igual.

¿Qué pasa si el padre/madre desea recuperar a su bebé?

Los padres que cambien de opinión pueden comenzar el proceso de reclamar a su recién nacido dentro de los 14 días. Estos padres deberán llamar al Departamento de Servicios para Niños y Familias (Department of Children and Family Services) del Condado de Los Angeles al 1-800-540-4000.

¿Sólo los padres podrán llevar al recién nacido?

No. Si bien en la mayoría de los casos son los padres los que llevan al bebé, la ley permite que otras personas lo hagan si tienen custodia legal.

¿Los padres o el adulto que entrega al bebé deben llamar antes de llevar al bebé?

No. El padre/madre o adulto puede llevar al bebé en cualquier momento, las 24 horas del día, los 7 días de la semana, siempre y cuando entreguen a su bebé a un empleado del hospital o cuartel de bomberos.

¿Es necesario que el padre/madre o adulto diga algo a las personas que reciben al bebé?

No. Sin embargo, el personal del hospital o cuartel de bomberos le pedirá a la persona que entregue al bebé que llene un cuestionario con la finalidad de recabar antecedentes médicos importantes, que resultan de gran utilidad para cuidar bien del bebé. El cuestionario incluye un sobre con el sello postal pagado para enviarlo en otro momento.

¿Qué pasará con el bebé?

El bebé será examinado y le brindarán atención médica. Cuando le den el alta del hospital, los trabajadores sociales inmediatamente ubicarán al bebé en un hogar seguro donde estará bien atendido, y se comenzará el proceso de adopción.

¿Qué pasará con el padre/madre o adulto que entregue al bebé?

Una vez que los padres o adulto hayan entregado al bebé al personal del hospital o cuartel de bomberos, pueden irse en cualquier momento.

¿Por qué se está haciendo esto en California?

La finalidad de la Ley de Entrega de Bebés sin Peligro es proteger a los bebés para que no sean abandonados, lastimados o muertos por sus padres. Usted probablemente haya escuchado historias trágicas sobre bebés abandonados en basureros o en baños públicos. Los padres de esos bebés probablemente hayan estado pasando por dificultades emocionales graves. Las madres pueden haber ocultado su embarazo, por temor a lo que pasaría si sus familias se enteraran. Abandonaron a sus bebés porque tenían miedo y no tenían nadie a quien pedir ayuda. El abandono de un recién nacido es ilegal y pone al bebé en una situación de peligro extremo. Muy a menudo el abandono provoca la muerte del bebé. La Ley de Entrega de Bebés sin Peligro impide que vuelva a suceder esta tragedia en California.

Historia de un bebé

A la mañana temprano del día 9 de abril de 2005, se entregó un recién nacido saludable a las enfermeras del Harbor-UCLA Medical Center. La mujer que llevó el recién nacido al hospital se dio a conocer como la tía del bebé, y dijo que la madre le había pedido que llevara al bebé al hospital en su nombre. Le entregaron a la tía un brazaletes con un número que coincidía con la pulsera del bebé; esto serviría como identificación en caso de que la madre cambiara de opinión con respecto a la entrega del bebé y decidiera recuperarlo dentro del período de 14 días que permite esta ley. También le dieron a la tía un cuestionario médico, y ella dijo que la madre lo llenaría y lo enviaría de vuelta dentro del sobre con franqueo pagado que le habían dado. El personal médico examinó al bebé y se determinó que estaba saludable y a término. El bebé fue ubicado con una buena familia que ya había sido aprobada para adoptarlo por el Departamento de Servicios para Niños y Familias.



EXHIBIT J

SOURCE CODE ESCROW AGREEMENT

FOR

MBIS SOLUTION

***(SAMPLE)**

*** ESCROW AGENT AND SPECIFIC TERMS SHALL BE FINALIZED AND MUTUALLY AGREED UPON BY THE
PARTIES PURSUANT TO THE TERMS OF THE AGREEMENT**

SAMPLE



Single Licensee
Software Escrow Agreement

Date	
Licensors	[Licensorname]
Licensee	[Licenseename]
Agreement Number	[Agreement#]

Notice: The parties to this Agreement are obliged to inform Escrow Agent of any changes to the Software or in their circumstances (including change of name, principal office, contact details or change of owner of the intellectual property in the Software).

SAMPLE

Escrow Agreement Dated:

Between:

- (1) [Licensorname] whose principal office is at [Licensoraddress] ("Licensor");
- (2) [Licenseename] whose principal office is at [Licenseeaddress] ("Licensee"); and
- (3) NCC Group Escrow Associates, LLC, a corporation organized and existing under the laws of Georgia with an office at 123 Mission Street, Suite 1020, San Francisco, CA 94105 USA ("Escrow Agent").

Background:

- (A) Licensee has been granted a license to use the Software which comprises computer programs.
- (B) Certain technical information and/or documentation relating to the Software is the confidential information and intellectual property of Licensor or a third party.
- (C) Licensor acknowledges that in certain circumstances, such information and/or documentation would be required by Licensee in order for it to continue to exercise its rights under its License Agreement with the Licensor.
- (D) The parties therefore agree that such information and/or documentation should be placed with a trusted third party, Escrow Agent, so that such information and/or documentation can be released to Licensee should certain circumstances arise.

Agreement:

In consideration of the mutual undertakings and obligations contained in this Agreement, the parties agree that:

1. Definitions and Interpretation

1.1 In this Agreement the following terms shall have the following meanings:

"**Agreement**" means the terms and conditions of this single licensee software escrow agreement set out below, including the Schedule(s) hereto.

"**Confidential Information**" means all technical and/or commercial information not in the public domain and which is designated in writing as confidential by any party.

"**Deposit Form**" means the form at Schedule 1 which is to be completed by Licensor and delivered to Escrow Agent with each deposit of the Escrow Material.

"**Escrow Material**" means the Source Code of the Software and such other material and documentation (including updates and upgrades thereto and new versions thereof) as are necessary to be delivered or deposited to comply with Clause 2 of this Agreement.

"**Full Verification**" means the tests and processes forming Escrow Agent's Full Verification service and/or such other tests and processes as may be agreed between the parties for the verification of the Escrow Material.

"**Integrity Testing**" means those tests and processes forming Escrow Agent's Integrity Testing service, in so far as they can be applied to the Escrow Material.

"**Intellectual Property Rights**" mean any copyright, patents, design patents, registered designs, design rights, utility models, trademarks, service marks, trade secrets, know how, database rights, moral rights, confidential information, trade or business names, domain names, and any other rights of a similar nature including industrial and proprietary rights and other similar protected rights in any country or jurisdiction together with all registrations, applications to register and rights to apply for registration of any of the aforementioned rights and any licenses of or in respect of such rights.

"**License Agreement**" means the agreement under which Licensee was granted a license to use the Software.

"**Order Form**" means the order form setting out the details of the order placed with Escrow Agent for setting up this Agreement.

"**Release Purposes**" means the purposes of understanding, maintaining, modifying and correcting the Software exclusively for and on behalf of Licensee together with such other purposes (if any) as are permitted under the License Agreement.

"**Software**" means the software together with any updates and upgrades thereto and new versions thereof licensed to Licensee under the License Agreement details of which are set out in Schedule 1.

"**Source Code**" means the computer programming code of the Software in human readable form.

1.2 This Agreement shall be interpreted in accordance with the following:

1.2.1 headings are for ease of reference only and shall not be taken into consideration in the interpretation of this Agreement;

1.2.2 all references to Clauses and Schedules are references to Clauses and Schedules of this Agreement; and

1.2.3 all references to a party or parties are references to a party or parties to this Agreement.

2. Licensor's Duties and Warranties

- 2.1 Licensor shall:
 - 2.1.1 deliver a copy of the Escrow Material to Escrow Agent within 30 days of the date of this Agreement;
 - 2.1.2 deliver an update or replacement copy of the Escrow Material to Escrow Agent within 30 days of a material update, error correction, enhancement, maintenance release or functional modification to the Software which results in an updated delivery of the object code version of the Software to Licensee;
 - 2.1.3 ensure that each copy of the Escrow Material deposited with Escrow Agent comprises the Source Code of the latest version of the Software used by Licensee;
 - 2.1.4 deliver to Escrow Agent an update or replacement copy of the Escrow Material within 30 days after the anniversary of the last delivery of the Escrow Material to ensure that the Escrow Material represents the most current version of Source Code and that the integrity of the Escrow Material media is maintained;
 - 2.1.5 deliver with each deposit of the Escrow Material a Deposit Form which includes the following information:
 - 2.1.5.1 details of the deposit including the full name of the Software (i.e. the original name as set out under Schedule 1 together with any new names given to the Software by Licensor), version details, media type, backup command/software used, compression used, archive hardware and operating system details; and
 - 2.1.5.2 password/encryption details required to access the Escrow Material;
 - 2.1.6 deliver with each deposit of the Escrow Material the following technical information (where applicable):
 - 2.1.6.1 documentation describing the procedures for building, compiling and installing the Software, including names and versions of the development tools;
 - 2.1.6.2 Software design information (e.g. module names and functionality); and
 - 2.1.7 deposit a detailed list of the suppliers of any third party software or tools, including open source software and tools, required to access, install, build or compile or otherwise use the Escrow Material.
- 2.2 Licensor warrants to both Escrow Agent and Licensee at the time of each deposit of the Escrow Material with Escrow Agent that:
 - 2.2.1 it has the full right, ability and authority to deposit the Escrow Material;
 - 2.2.2 in entering into this Agreement and performing its obligations under it, it is not in breach of any of its ongoing express or implied obligations to any third party(s); and
 - 2.2.3 the Escrow Material deposited under Clause 2.1 contains all information in human-readable form and is on suitable media to enable a reasonably skilled programmer or analyst to understand, maintain, modify and correct the Software.

3. Licensee's Responsibilities and Undertakings

- 3.1 Licensee shall notify Escrow Agent of any change to the Software that necessitates a replacement deposit of the Escrow Material.
- 3.2 In the event that the Escrow Material is released under Clause 6, Licensee shall:
 - 3.2.1 keep the Escrow Material confidential at all times;
 - 3.2.2 use the Escrow Material only for the Release Purposes;
 - 3.2.3 not disclose the Escrow Material to any person save such of Licensee's employees or contractors who need to know the same for the Release Purposes. In the event that Escrow Material is disclosed to its employees or contractors, Licensee shall ensure that they are bound by the same confidentiality obligations as are contained in this Clause 3.2;
 - 3.2.4 hold all media containing the Escrow Material in a safe and secure environment when not in use; and
 - 3.2.5 forthwith destroy the Escrow Material should Licensee cease to be entitled to use the Software under the terms of the License Agreement.

4. Escrow Agent's Duties

- 4.1 Escrow Agent shall:
 - 4.1.1 at all times during the term of this Agreement, retain the Escrow Material in a safe and secure environment; and
 - 4.1.2 inform Licensor and Licensee of the receipt of any deposit of the Escrow Material by sending to both parties a copy of the Deposit Form, and/or the Integrity Testing report or Full Verification report (as the case may be) generated from the testing processes carried out under Clause 10.

SAMPLE

- 4.2 In the event of failure by Licensor to deposit any Escrow Material with Escrow Agent, Escrow Agent shall not be responsible for procuring such deposit and may, at its sole discretion, notify the Licensor and Licensee of Licensor's failure to deposit any Escrow Material.
- 4.3 Escrow Agent may appoint agents, contractors or sub-contractors as it deems fit to carry out the Integrity Testing and the Full Verification processes. Escrow Agent shall ensure that any such agents, contractors and sub-contractors are bound by the same confidentiality obligations as are contained in Clause 8.
- 4.4 Escrow Agent has the right to make such copies of the Escrow Material as may be necessary solely for the purposes of this Agreement.

5. Payment

- 5.1 The parties shall pay Escrow Agent's fees and charges as published from time to time or as otherwise agreed, as listed in the Order Form. Escrow Agent's fees as published are exclusive of any applicable sales tax.
- 5.2 If Escrow Agent is required to perform any additional or extraordinary services as a result of being an escrow agent including intervention in any litigation or proceeding, Escrow Agent shall receive reasonable compensation for such services and be reimbursed for all costs incurred, including reasonable attorney's fees.
- 5.3 Escrow Agent shall be entitled to review and vary its standard fees and charges for its services under this Agreement from time to time but no more than once a year and only upon 45 days written notice to the parties.
- 5.4 All invoices are payable within 30 days from the date of invoice. Interest shall accrue at the lesser of 1.5% per month or the maximum amount permitted by applicable law for any fees that are undisputed by the paying party and remain unpaid for more than 30 days past the due date of the applicable invoice.
- 5.5 In the event of a dispute made in good faith as to the amount of fees, the party responsible for payment agrees to remit payment on any undisputed amount(s) in accordance with Clause 5.1 above. In such circumstances, the interest on the fees shall not accrue as to any disputed amounts unless not paid within 30 days after such dispute has been resolved by the parties.

6. Release Events and Procedures

- 6.1 Subject to: (i) the remaining provisions of this Clause 6 and (ii) the receipt by Escrow Agent of the fees chargeable upon a release and any other fees and interest (if any) outstanding under this Agreement, Escrow Agent will release the Escrow Material to a duly authorized representative of Licensee if any of the following events ("**Release Event(s)**") occur:
 - 6.1.1 a receiver, trustee, or similar officer is appointed for the business or property of Licensor; or
 - 6.1.2 Licensor files a petition in bankruptcy, files a petition seeking any reorganization (without confirming immediately in writing to Licensee that it will continue to maintain the Software in accordance with the terms of the License Agreement or any applicable maintenance agreement), makes an arrangement, composition, or similar relief under any law regarding insolvency or relief for debtors, or makes an assignment for the benefit of creditors; or
 - 6.1.3 any involuntary petition or proceeding under bankruptcy or insolvency laws is instituted against Licensor and not stayed, enjoined, or discharged within 60 days; or
 - 6.1.4 Licensor takes any corporate action authorizing any of the foregoing; or
 - 6.1.5 any similar or analogous proceedings or event to those in Clauses 6.1.1 to 6.1.3 above occurs in respect of Licensor within any jurisdiction outside the USA; or
 - 6.1.6 Licensor ceases to carry on its business or the part of its business which relates to the Software; or
 - 6.1.7 Licensor or, where relevant, its agent, parent, subsidiary or associated company is in material breach of its obligations as to maintenance or modification of the Software under the License Agreement or any maintenance agreement entered into in connection with the Software and has failed to remedy such default notified by Licensee to Licensor within the time period specified in the License Agreement or any maintenance agreement or other relevant agreement, and if no time period is specified, within a commercially reasonable time period.
- 6.2 Licensee must notify Escrow Agent and Licensor of the Release Event specified in Clause 6.1 by delivering to Escrow Agent a notice in writing ("**Notice**") declaring that such Release Event has occurred, setting out the facts and circumstances of the Release Event, that the License Agreement and any maintenance agreement, if relevant, for the Software was still valid and effective up to the occurrence of such Release Event and exhibiting such documentary evidence in support of the Notice as Escrow Agent shall reasonably require.
- 6.3 Upon receipt of a Notice from Licensee claiming that a Release Event has occurred:
 - 6.3.1 Escrow Agent shall submit a copy of the Notice to Licensor (with a copy to the Licensee in order to acknowledge receipt of the Notice) by courier or other form of guaranteed delivery; and
 - 6.3.2 unless within 14 calendar days after the date of dispatch of the Notice by Escrow Agent, Escrow Agent receives a counter-notice in writing from Licensor stating that in their view no such Release Event has occurred or, if appropriate, that the event or circumstance giving rise to the Release Event has been rectified as shown by

SAMPLE

documentation in support thereof, Escrow Agent will release the Escrow Material to Licensee for its use for the Release Purposes.

- 6.4 Upon receipt of the counter-notice from Licenser under Clause 6.3.2, Escrow Agent shall send a copy of the counter-notice and any supporting evidence to Licensee (with a copy to Licenser in order to acknowledge receipt of the counter-notice) by courier or other form of guaranteed delivery.
- 6.5 Within 90 calendar days of dispatch of the counter-notice by Escrow Agent, Licensee may give Licenser and Escrow Agent written notice of its intention to arbitrate under Clause 7 ("Demand").
- 6.6 If, within 90 calendar days of dispatch of the counter-notice by Escrow Agent to Licensee, Licensee has not given a Demand to Licenser and Escrow Agent, the Notice submitted by Licensee will be deemed to be no longer valid and Licensee shall be deemed to have waived their right to release of the Escrow Material for the particular reason or event specified in the original Notice. In such circumstances, this Agreement shall continue in full force and effect.

7. Disputes regarding Release Event(s)

- 7.1 All disputes regarding whether the Release Event(s) specified in the Notice occurred before the Licensee delivered the Notice to Escrow Agent shall be decided by one (1) arbitrator. The place of the arbitration shall be San Francisco, California. If the Licenser and Licensee have not agreed on an arbitrator within seven (7) days after the Licenser receives the Demand, the American Arbitration Association (AAA) shall appoint an arbitrator within ten (10) days of receipt of a request to appoint an arbitrator, which may be filed by either the Licenser or Licensee. The arbitrator's agreement to the deadlines set forth in this Clause 7 shall be a condition to the appointment as arbitrator, but failure to adhere to these time limits shall not be a basis for challenging the award.
- 7.2 Within seven (7) days of the appointment of the arbitrator, the Licenser and Licensee shall each provide written submissions to the arbitrator, together with all documentary evidence in their possession in support of their claim.
- 7.3 Based solely on the written submissions of the Licenser and Licensee, and without the need for a hearing, the arbitrator shall render and deliver his or her award to the Licenser, the Licensee and Escrow Agent within fourteen (14) days of receiving the written submissions from the Licenser and Licensee. The Licensee and Licenser may agree to extend this time limit or the arbitrator may do so in its discretion if he or she determines that the interest of justice so requires.
- 7.4 The award shall be limited to a determination of whether or not there existed a Release Event at the time Licensee delivered the Notice to Escrow Agent and, where the Licenser claims within the timescales specified in Clause 6.3.2 that the Release Event has been rectified and the Licensee does not agree, to a determination of whether or not the Release Event has in fact been rectified. In addition, the arbitrator shall award the prevailing party its attorneys' fees and costs, including the fees and costs of the arbitrator.
- 7.5 The arbitral award shall be final and binding upon the Parties hereto. If the arbitrator finds that a Release Event existed at the time of delivery of the Notice to Escrow Agent, Escrow Agent is hereby authorized to release and deliver the Escrow Material to the Licensee within 5 working days of the decision being notified by the arbitrator to the parties. If the arbitrator finds to the contrary, then Escrow Agent shall not release the Escrow Material and shall continue to hold the Escrow Material in accordance with the terms of this Agreement.
- 7.6 The Parties agree that the arbitration provided in this Clause 7 shall not be consolidated or joined with any other proceeding regarding disputes between or among any of the Parties.

8. Confidentiality

- 8.1 The Escrow Material shall remain at all times the confidential and intellectual property of its owner.
- 8.2 In the event that Escrow Agent releases the Escrow Material to Licensee, Licensee shall be permitted to use the Escrow Material only for the Release Purposes.
- 8.3 Subject to Clause 8.4, Escrow Agent agrees to keep all Confidential Information relating to the Escrow Material and/or the Software that comes into its possession or to its knowledge under this Agreement in strict confidence and secrecy. Escrow Agent further agrees not to make use of such information and/or documentation other than for the purposes of this Agreement and, unless the parties should agree otherwise in writing and subject to Clause 8.4, will not disclose or release it other than in accordance with the terms of this Agreement.
- 8.4 Escrow Agent may release the Escrow Material to the extent that it is required by applicable federal, state or local law, regulation, court order, judgment, decree or other legal process, provided that, unless prohibited by the terms of the order or the relevant law or regulation, Escrow Agent has notified Licenser and Licensee prior to such required release, has given Licenser and/or Licensee an opportunity to contest (at their own expense) such required release, within the time parameters mandated by such applicable regulation, court order, judgment, decree or other legal process. Escrow Agent is hereby expressly authorized in its sole discretion to obey and comply with all orders, judgments, decrees so entered or issued by any court, without the necessity of inquiring as to the validity of such order, judgment or decree, or the court's underlying jurisdiction. Where Escrow Agent obeys or complies with any such order, judgment or decree, Escrow Agent shall not be liable to Licensee, Licenser or any third party by reason of such compliance, notwithstanding that such order, judgment or decree may subsequently be reversed, modified or vacated.

9. Intellectual Property Rights

- 9.1 The release of the Escrow Material to Licensee will not act as an assignment of any Intellectual Property Rights that Licensor or any third party possesses in the Escrow Material. However, upon deposit of the Escrow Material, the title to the media upon which the Escrow Material is deposited ("**Media**") is transferred to Escrow Agent. Upon delivery of the Escrow Material back to Licensor, the title to the Media shall transfer back to the Licensor. If the Escrow Material is released to the Licensee, the title to the Media shall transfer to the Licensee.
- 9.2 The Intellectual Property Rights in the Integrity Testing report and any Full Verification report shall remain vested in Escrow Agent. Licensor and Licensee shall each be granted a non-exclusive right and license to use such report for the purposes of this Agreement and their own internal purposes only.

10. Integrity Testing and Full Verification

- 10.1 Escrow Agent shall bear no obligation or responsibility to any party to this Agreement or person, firm, company or entity whatsoever to determine the existence, relevance, completeness, accuracy, operation, effectiveness, functionality or any other aspect of the Escrow Material received by Escrow Agent under this Agreement.
- 10.2 As soon as practicable after the Escrow Material has been deposited with Escrow Agent, Escrow Agent shall apply its Integrity Testing processes to the Escrow Material.
- 10.3 Any party to this Agreement shall be entitled to require Escrow Agent to carry out a Full Verification. Subject to Clause 10.4, Escrow Agent's prevailing fees and charges for the Full Verification processes and all reasonable expenses incurred by Escrow Agent in carrying out the Full Verification processes shall be payable by the requesting party.
- 10.4 If the Escrow Material fails to satisfy Escrow Agent's Full Verification tests within the timescales originally provided for the completion of the Full Verification test as a result of being defective or incomplete in content, Escrow Agent's fees, charges and expenses in relation to the Full Verification tests shall be paid by Licensor.
- 10.5 Should the Escrow Material deposited fail to satisfy Escrow Agent's Integrity Testing or Full Verification tests under Clauses 10.2 or 10.3, Licensor shall, within 14 days of the receipt of the notice of test failure from Escrow Agent, deposit such new, corrected or revised Escrow Material as shall be necessary to ensure its compliance with its warranties and obligations in Clause 2. If Licensor fails to make such deposit of the new, corrected or revised Escrow Material, Escrow Agent will issue a report to Licensee (with a copy to Licensor) detailing the problem with the Escrow Material as revealed by the relevant tests.

11. Escrow Agent's Liability

- 11.1 Nothing in this Clause 11 excludes or limits the liability of Escrow Agent for gross negligence or intentional misconduct.
- 11.2 Subject to Clause 11.1, Escrow Agent shall not be liable for:
 - 11.2.1 any loss or damage caused to either Licensor or Licensee except to the extent that such loss or damage is caused by the negligent acts or omissions of or a breach of any contractual duty by Escrow Agent, its employees, agents or sub-contractors and in such event Escrow Agent's total liability with regard to all claims arising under or by virtue of this Agreement or in connection with the performance or contemplated performance of this Agreement, shall not exceed the sum of \$250,000 (two hundred and fifty thousand US dollars); and
 - 11.2.2 any special, indirect, incidental or consequential damages whatsoever.
- 11.3 Escrow Agent shall not be responsible in any manner whatsoever for any failure or inability of Licensor or Licensee to perform or comply with any provision of this Agreement.
- 11.4 Escrow Agent shall not be liable in any way to Licensor or Licensee for acting in accordance with the terms of this Agreement and specifically (without limitation) for acting upon any notice, written request, waiver, consent, receipt, statutory declaration or any other document furnished to it pursuant to and in accordance with this Agreement.
- 11.5 Escrow Agent shall not be required to make any investigation into and shall be entitled in good faith without incurring any liability to Licensor or Licensee to assume (without requesting evidence thereof) the validity, authenticity, veracity and due and authorized execution of any documents, written requests, waivers, consents, receipts, statutory declarations or notices received by it in respect of this Agreement.

12. Indemnity

- 12.1 Save for any claim falling within the provisions of Clause 11.1, the Licensor and the Licensee jointly and severally agree at all times to indemnify and hold harmless Escrow Agent in respect of all of its legal and all other costs (including reasonable attorney's fees), fees and expenses incurred directly or indirectly as a result of being brought into or otherwise becoming involved in any form of dispute resolution proceedings or any litigation of any kind between the Licensor and the Licensee in relation to this Agreement to the extent that this Agreement does not otherwise provide for reimbursement of such costs.
- 12.2 The Licensor shall assume all liability and shall at all times indemnify and hold harmless Escrow Agent and its officers, agents, sub-contractors and employees from and against any and all liability, loss, damages, costs, legal costs (including reasonable attorney's fees), professional and other expenses and any other liabilities of whatever nature, awarded against or agreed to be paid or otherwise suffered, incurred or sustained by Escrow Agent, whether direct, indirect or consequential as a result of or in connection with any claim by any third party(s) for alleged or actual

SAMPLE

infringement of Intellectual Property Rights arising out of or in connection with all and any acts or omissions of Escrow Agent in respect of the Escrow Material as contemplated under this Agreement.

13. Term and Termination

- 13.1 This Agreement shall continue until terminated in accordance with this Clause 13.
- 13.2 Licensee may terminate this Agreement at any time by giving sixty (60) days prior written notice to Escrow Agent. Upon such termination, Escrow Agent shall, unless it receives written instructions to the contrary from the Licensor within 30 days of the date of termination, destroy the Escrow Material.
- 13.3 If the License Agreement has expired or has been lawfully terminated, then Licensee shall give notice to Escrow Agent within 14 days thereof to terminate this Agreement, failing which, Licensor shall be entitled to give written notice to Escrow Agent to terminate this Agreement. Upon receipt of such a notice from Licensor, Escrow Agent shall notify Licensee of Licensor's notice to terminate. Unless within 30 days of Escrow Agent giving such notice to Licensee, Escrow Agent receives a counter-notice from Licensee disputing the termination of the License Agreement, then Licensee shall be deemed to have consented to such termination and this Agreement shall immediately automatically terminate. Any disputes arising under this Clause shall be dealt with in accordance with the dispute resolution procedure in Clause 7. Upon termination under this Clause, Escrow Agent shall destroy the Escrow Material.
- 13.4 Subject to Clause 13.3, Licensor may only terminate this Agreement with the written consent of Licensee.
- 13.5 This Agreement shall automatically immediately terminate upon release of the Escrow Material to Licensee in accordance with Clause 6.
- 13.6 If Licensor or Licensee, as the case may be, fails to pay an invoice addressed to it for services under this Agreement in accordance with the terms of Clause 5, Escrow Agent reserves the right to give that party written notice to pay the outstanding invoice within 30 days. If Licensor has not paid its invoice by the expiry of the 30 day notice period, Escrow Agent will give Licensee a period of 30 days to pay Licensor's invoice. If Licensor or Licensee (as appropriate) has not paid its invoice after being given notice in accordance with this Clause, Escrow Agent shall have the right to terminate this Agreement without further notice. Any amounts owed by Licensor but paid by Licensee will be recoverable by Licensee direct from Licensor as a debt and, if requested, Escrow Agent shall provide appropriate documentation to assist in such recovery.
- 13.7 Upon termination under the provisions of Clauses 13.4 or 13.6 and in the event of termination under Clause 13.5 where Licensee does not require release of all of the Escrow Material, for 30 days from the date of termination Escrow Agent will make the Escrow Material available for collection by Licensor or its agents from the premises of Escrow Agent during office hours. After such 30 day period Escrow Agent has the authority to destroy the Escrow Material.
- 13.8 Notwithstanding any other provision of this Clause 13, Escrow Agent may resign as escrow agent hereunder and terminate this Agreement by giving sixty (60) days written notice to Licensor and Licensee ("**Resignation Notice**"). In that event, Licensor and Licensee shall have the option to appoint a mutually acceptable new custodian on similar terms and conditions to those contained herein. If a new custodian is not appointed within fourteen (14) days of delivery of the Resignation Notice or a longer period as agreed by Licensor and Licensee, Licensor or Licensee shall be entitled to request the American Arbitration Association to appoint a suitable new custodian upon terms and conditions consistent with those in this Agreement. Such appointment shall be final and binding on Licensor and Licensee. If Escrow Agent is notified of the new custodian sixty (60) days of giving the Resignation Notice, Escrow Agent will forthwith deliver the Escrow Material to the new custodian. If Escrow Agent is not notified of the new custodian within the aforementioned notice period, Escrow Agent will destroy the Escrow Material.
- 13.9 The provisions of Clauses 1, 3.2, 5, 8, 9, 10.1, 11, 12, 13.9 to 13.11 (inclusive) and 14 shall continue in full force after termination of this Agreement.
- 13.10 On and after termination of this Agreement, Licensor and/or Licensee (as appropriate) shall remain liable to Escrow Agent for payment in full of any fees and interest which have become due but which have not been paid as at the date of termination.
- 13.11 The termination of this Agreement, however arising, shall be without prejudice to the rights accrued to the parties prior to termination.

14. General

- 14.1 A party shall notify the other parties to this Agreement, within 30 days of its occurrence, of any of the following:
 - 14.1.1 a change of its name, principal office, contact address or other contact details; and
 - 14.1.2 any material change in its circumstances that may affect the validity or operation of this Agreement.
- 14.2 This Agreement shall be deemed entered into in California and will be governed by and construed according to the laws of the state of California, excluding that body of law known as conflict of law. The parties agree that any dispute arising under this Agreement, except as provided in Clause 7, will be resolved in the state or federal courts in San Francisco, California, and the parties hereby expressly consent to the jurisdiction thereof.
- 14.3 This Agreement, together with the Order Form and any relevant Escrow Agent standard terms and conditions including Escrow Agent escrow terms and conditions and, where applicable, Escrow Agent verification terms and conditions represent the whole agreement relating to the escrow arrangements between Escrow Agent and the other parties for the Software and shall supersede all prior agreements, discussions, arrangements, representations, negotiations and

SAMPLE

undertakings. In the event of any conflict between any of these documents, the terms of this Agreement shall prevail.

- 14.4 Unless the provisions of this Agreement otherwise provide, any notice or other communication required or permitted to be given or made in writing hereunder shall be validly given or made if delivered by hand or courier or if dispatched by certified or registered mail (airmail if overseas) addressed to the address specified for the parties in this Agreement (or such other address as may be notified to the parties from time to time) or if sent by facsimile message to such facsimile number as has been notified to the parties from time to time and shall be deemed to have been received:
- (i) if delivered by hand or courier, at the time of delivery;
 - (ii) if sent by certified or registered mail (airmail if overseas), 3 business days after posting (6 days if sent by airmail);
 - (iii) if sent by facsimile, at the time of completion of the transmission of the facsimile with facsimile machine confirmation of transmission to the correct facsimile number of all pages of the notice.
- 14.5 Except where any party merges, is acquired or has substantially all of its assets acquired and the new entity or acquirer agrees to assume all of their obligations and liabilities under this Agreement, no party shall assign, transfer or subcontract this Agreement or any rights or obligations hereunder without the prior written consent of the other parties.
- 14.6 This Agreement shall be binding upon and survive for the benefit of the successors in title and permitted assigns of the parties.
- 14.7 If any provision of this Agreement is declared too broad in any respect to permit enforcement to its full extent, the parties agree that such provision shall be enforced to the maximum extent permitted by law and that such provision shall be deemed to be varied accordingly. If any provision of this Agreement is found by any court, tribunal or administrative body of competent jurisdiction to be wholly or partly illegal, invalid, void or unenforceable, it shall, to the extent of such illegality, invalidity or unenforceability, be deemed severable and the remaining part of the provision and the rest of the provisions of this Agreement shall continue in full force and effect.
- 14.8 Save as expressly provided in this Agreement, no amendment or variation of this Agreement shall be effective unless in writing and signed by a duly authorized representative of each of the parties to it.
- 14.9 The parties shall not be liable to each other or be deemed to be in breach of this Agreement by reason of any delay in performing, or failure to perform, any of their obligations under this Agreement if the delay or failure was for a reason beyond that party's reasonable control (including, without limitation, fire, flood, explosion, epidemic, riot, civil commotion, any strike, lockout or other industrial action, act of God, war or warlike hostilities or threat of war, terrorist activities, accidental or malicious damage, or any prohibition or restriction by any governments or other legal authority which affects this Agreement and which is not in force on the date of this Agreement). A party claiming to be unable to perform its obligations under this Agreement (either on time or at all) in any of the circumstances set out above must notify the other parties of the nature and extent of the circumstances in question as soon as practicable. If such circumstances continue for more than six months, any of the other parties shall be entitled to terminate this Agreement by giving one month's notice in writing.
- 14.10 No waiver by any party of any breach of any provisions of this Agreement shall be deemed to be a waiver of any subsequent or other breach and, subject to Clause 6.6, no failure to exercise or delay in exercising any right or remedy under this Agreement shall constitute a waiver thereof.
- 14.11 This Agreement may be executed in any number of counterparts and by different parties in separate counterparts. Each counterpart when so executed shall be deemed to be an original and all of which together shall constitute one and the same agreement.

SAMPLE

Signed for and on behalf of [Licensorname]

Name: |

Position: | (Authorized Signatory)

Signed for and on behalf of [Licenseename]

Name: |

Position: | (Authorized Signatory)

Signed for and on behalf of NCC Group Escrow Associates, LLC

Name: |

Position: | (Authorized Signatory)

SAMPLE

Schedule 1 (Deposit Form)

ESCROW MATERIALS DEPOSIT FORM	
Escrow Account Number:	[Agreement Number]
Product Name:	[Software Name]
Date:	

DEPOSITOR DETAILS

Company Name:		Technical Contact:	
Address:		Signature:	
		Position:	
Telephone No:		Email Address:	

MATERIAL DETAILS

Media Type (e.g. Disc, Tape etc.)	Number of media items	Name of Software	Version/Release
Hardcopy Documents (please supply details):			
Softcopy Documents (please give location on media, e.g. \docs\build):			
What Hardware was used to create the media deposit?			
What Operating System was used?			
What Backup Command/Software was used?			
What Software Compression has been used?			
What Encryption/Password Protection has been used?			
In what Development Language is the source code written?			
Approximate size of the data on the media in megabytes?			
Provide details of any third party software required to access/compile the material.			
Provide details of any additional build information.			

The following information MUST be provided for Escrow Agent to accept the deposit of escrow material:

If this is your initial/first deposit, please fill in Section 1.

If this is your second or subsequent deposit (i.e. a replacement/update) please fill in Section 2.

SECTION 1: Initial Deposit (First Deposit) – Is this a complete deposit? <input type="checkbox"/> YES <input type="checkbox"/> NO if NO, please indicate when the rest of the deposit will be sent _____
SECTION 2: Deposit Updates/Replacements – Is the deposit a complete replacement of any of the previous deposits? <input type="checkbox"/> YES <input type="checkbox"/> NO If YES, would you like the past deposit(s) to be: <input type="checkbox"/> RETAINED <input type="checkbox"/> RETURNED <input type="checkbox"/> DESTROYED *For returns and destroys, please specify which deposit(s) this applies to by reference to the month and year of delivery to Escrow Agent

Signature: _____ of Recipient: _____	Date material received by _____ Escrow Agent: _____
(Tick 'ALL' if all previous deposits): <input type="checkbox"/> All <input type="checkbox"/> SPECIFIC DEPOSIT(S):	

EXHIBIT K
THIRD PARTY SOFTWARE LICENSE TERMS
FOR
MBIS SOLUTION

ADOBE GENERAL TERMS OF USE

ADOBE GENERAL TERMS OF USE

Last updated October 16, 2012. Replaces the May 7, 2012 version in its entirety.

1. Your Agreement With Adobe.

1.1 Choice of Law. If you are a resident of North America, your relationship is with Adobe Systems Incorporated, a United States company, and you agree to be bound by the laws of California and the laws of the United States. If you reside outside of North America, your relationship is with Adobe Systems Software Ireland Limited, and you agree to be bound by the laws of Ireland.

1.2 This document sets forth your legal agreement with Adobe Systems Incorporated or Adobe Systems Software Ireland Limited and its agents and affiliates (collectively, "Adobe"). Your use of any Adobe website or service (collectively "Service" or "Services") that references to these terms is subject to these Terms of Use (the "General Terms").

1.3 Some Services may also be subject to additional or different terms (the "Additional Terms").

1.4 If there is any conflict between the General Terms and the Additional Terms, then the Additional Terms take precedence in relation to that Service. The General Terms and any applicable Additional Terms and all other documents incorporated by reference in these General Terms are referred to as the "Terms".

1.5 Adobe may change the Terms at its sole discretion. If we change the Terms, then we will make a new copy available at <http://www.adobe.com/go/terms>. Your use of the Services is subject to the most current version of the Terms at the time of such use.

2. Definitions.

Unless otherwise defined, capitalized terms used throughout these General Terms have the meanings stated below:

2.1 "Account Information" means the information you provide to Adobe when you register for a service, including your Adobe ID and log-in information.

2.2 "Adobe Materials" means any Materials provided by Adobe under these Terms.

2.3 "Intellectual Property Rights" means copyright, moral rights, trademark, trade dress, patent, trade secret, unfair competition, and any other intellectual and proprietary rights.

2.4 "Law" means any applicable law, regulation, or generally accepted practices or guidelines in any applicable jurisdiction, such as any laws regarding the export of data or software to and from the United States or other applicable countries.

2.5 "Marks" means the trademarks, logos and service marks displayed on the Services.

2.6 "Materials" means any materials provided by you or Adobe, including without limitation any (a) User Material; (b) information, data, documents, images, photographs, graphics, audio, videos, or webcasts, (c) products, and (d) Software.

2.7 "Shared Material" means the User Material that you or other Users share through the Services.

2.8 "Share" means to email, post, transmit, upload, or otherwise make available through your use of the Services.

2.9 "Software" means Adobe software code and associated documentation, including without limitation any mobile and tablet applications related to the Services, content files, drivers, patches, or fonts.

2.10 "User" means a user of the Service.

2.11 "User Material" means (a) Your Material and (b) Shared Material uploaded by other Users.

2.12 "Your Material" means any Materials that you Share through your use of the Services.

2.13 "Your Shared Material" means Your Material that you choose to make into Shared Material.

3. Acceptance of Terms.

3.1 You may not use the Services if you do not agree to the Terms. You may accept the Terms (a) by selecting "I agree" to these Terms, (b) by using the Services in any way, such as downloading or uploading any Materials made available via the Services by Adobe, you, or other Users, or (c) by merely browsing the Services.

3.2 You may not use the Services if (a) you are prohibited by Law from receiving or using the Services, (b) you are not fully able and competent to enter into a binding contract with Adobe, such as if you are not of legal age or have not obtained parental consent. **In particular, unless expressly stated otherwise in the Additional Terms for any given Service, you affirm that you are over the age of 13 and acknowledge that these Services were not intended for children under 13.**

3.3 Adobe may require you to provide consent to the updated Terms before further use of the Services is permitted. Otherwise, your continual use of any Service constitutes your acceptance of the changes.

4. Privacy Policy.

For information about Adobe's data protection and collection practices, please read the Adobe Privacy Policy at <http://www.adobe.com/go/privacy>, which is incorporated herein by reference. You agree to Adobe's use of your data in accordance with the Privacy Policy.

5. Ownership.

5.1 Services and Adobe Materials. The Services and Adobe Materials, and their selection and arrangement, are protected by Intellectual Property Rights. Except as expressly provided in the Terms, Adobe and its licensors do not grant any express or implied rights to use the Services and Materials. All rights, title, and interest in the Service and Adobe Materials, in all languages, formats, and media throughout the world, are and will continue to be the exclusive property of Adobe and/or its licensors and nothing in the Terms shall be construed to confer any license or right, by implication, estoppel or otherwise, under copyright or other intellectual property rights, to you or any third party.

5.2 Trademarks. The Marks are the property of Adobe or other rights holders. You are not permitted to use the Marks without the prior consent of Adobe or the rights holder. Adobe and the Adobe logo are trademarks of Adobe Systems Incorporated. For a current list of Adobe's Marks, as well as certain third party Marks, please refer to the posted trademark information at <http://www.adobe.com/go/trademarks>.

6. Use of Service and Materials.

6.1 If you comply with the terms and conditions of this Agreement, Adobe grants to you a non-exclusive, non-transferable, revocable right to access and use the Services, to Share Your Materials to

the Service, and to use the Adobe Materials in connection with the Services, subject to the restrictions stated in this Section.

6.2 Except with respect to Your Material, you agree:

- (a) Not to alter, copy, modify, or re-transmit the Materials;
- (b) Not to lease, license, rent, or sell the Materials or the right to use and access the Services;
- (c) Not to remove, obscure, or alter any text or proprietary notices contained in Materials;
- (d) Not to copy or imitate part or all of the design, layout, or look-and-feel of the Service, which are protected by Intellectual Property Rights;
- (e) To use the Services and the Materials only as permitted by the Terms and any Law; and
- (f) That certain Services and Materials may be available only if you have paid a fee or have provided certain Account Information.

6.3 Adobe uses reasonable efforts to make the Services available 24 hours a day, 7 days a week. However, there will be occasions when the Service will be interrupted for maintenance, upgrades and repairs, or as a result of failure of telecommunications links and equipment that are beyond our control. Adobe will take reasonable steps to minimize such disruption, to the extent it is within our reasonable control. Certain Services may not be available in all languages.

6.4 Adobe may modify or discontinue, temporarily or permanently, the Services or Materials, or any portion thereof, with or without notice. You agree that Adobe shall not be liable to you or anyone else if we do so.

6.5 Payment Terms.

- (a) **Subscription Fees.** Certain Services require you to purchase a subscription or membership in order to access all or part of such Services. Subscription Fees are non-refundable, except as otherwise stated in specific subscription terms applicable to a Service. Subscription Fees may change at the end of your subscription period. Subscription terms are available at http://www.adobe.com/go/subscription_terms.
- (b) You are responsible for paying all taxes levied in connection with your use of the Services. Your credit card company or bank may impose on you other fees, such as foreign exchange fees, in connection with your payment of the Subscription Fees. Your ability to access the Services may require payment of third-party fees (such as telephone toll charges, mobile carrier fees, ISP, data plan, etc.). Adobe has no connection to or responsibility for such fees.
- (c) **Collection of Subscription Fee.** You agree that, in the event Adobe is unable to collect the Subscription Fees owed by you to Adobe for the Services, Adobe may take the steps it deems necessary to collect such Subscription Fees from you and that you will be responsible for all costs and expenses incurred by Adobe in connection with such collection activity.

7. Account Information; Personal URL.

7.1 You agree that your Account Information will always be complete, accurate, and up-to-date. It is your responsibility to keep your account password or log-in credentials confidential at all times and you are solely responsible to Adobe for all activity that occurs via your Account. If you become aware of any unauthorized use of your account or Account Information, or any other breach of security, you

agree to notify Adobe by contacting Support at http://www.adobe.com/go/support_contact. Adobe may require that you change your Account Information or certain parts of your Account Information at any time for any reason. Unless Adobe expressly allows you the right to create and manage Adobe IDs as an account administrator for a company or unless expressly permitted in the Additional Terms, you may not use another person's Account Information.

7.2 As part of registering for a Service, Adobe may require you to create a unique URL, such as `your_name_here.adobe.com`. Such unique URL may be used solely with the Service, only for so long as you maintain a valid account and shall not be used for any other purpose. Adobe may revoke your right to use that URL for any reason deemed appropriate by Adobe in its sole discretion by giving you at least thirty days prior notice of such revocation, except in the event that your URL, or content therein, is determined by Adobe in its sole discretion to contain infringing or illegal content or content that otherwise violates the Terms. In such event, Adobe reserves the right to revoke your right to use your unique URL immediately without notice. Additionally, Adobe owns and retains all right, title, and interest in and to the use of "Adobe," and other Adobe property in association with a User's unique URL. Upon termination for any reason, Adobe may permit another User to use the unique URL previously selected by you.

8. User Conduct.

8.1 You agree not to access or attempt to access the Services by any means other than the interface provided by Adobe or circumvent any access or use restrictions put into place to prevent certain uses of the Services.

8.2 You agree not to use, or to encourage or permit others to use, the Services to:

- (a) Share any Material that is unlawful, harmful, threatening, abusive, tortious, defamatory, libelous, vulgar, obscene, child pornographic, lewd, profane, invasive of another's privacy, hateful, or racially, ethnically, or otherwise objectionable;
- (b) Stalk, intimidate, and/or harass another;
- (c) Incite others to commit violence;
- (d) Harm minors in any way;
- (e) Share any Material that you do not have a right to Share under any Law or contractual or fiduciary relationship;
- (f) Share any Material that infringes any Intellectual Property Right or other proprietary right of any party; (g) Impersonate any person or entity, or falsely state or otherwise misrepresent your affiliation with a person or entity;
- (h) Forge headers or otherwise manipulate identifiers to disguise the origin of any of Materials posted on or transmitted through the Services;
- (i) Use the Services or Materials such that it will mislead a User into believing that they are interacting directly with Adobe or any Service;
- (j) Engage in any chain letters, contests, junk email, pyramid schemes, spamming, surveys, or other duplicative or unsolicited messages (commercial or otherwise);
- (k) Use any Adobe domain name as a pseudonymous return email address;

- (l) Share any Material that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment;
- (m) Access or use the Services in any manner that could damage, disable, overburden, or impair any Adobe server or the networks connected to any Adobe server;
- (n) Intentionally or unintentionally interfere with or disrupt the Services or violate any applicable Laws related to the access to or use of the Services, violate any requirements, procedures, policies, or regulations of networks connected to the Services, or engage in any activity prohibited by the Terms;
- (o) Disrupt or interfere with the security of, or otherwise cause harm to, the Services, Materials, systems resources, accounts, passwords, servers, or networks connected to or accessible through the Services or any affiliated or linked sites;
- (p) Disrupt, interfere with, or inhibit any other User from using and enjoying the Services or Materials, or other affiliated or linked sites, Services, or Materials;
- (q) Access or attempt to access any Material that you are not authorized to access or through any means not intentionally made available through the Services;
- (r) Market any goods or services for any business purposes (including advertising and making offers to buy or sell goods or services), unless specifically allowed to do so by Adobe;
- (s) Reproduce, sell, trade, resell or exploit for any commercial purpose, any portion of the Services or any Materials, use of any Service or Materials, or access to any Service or Materials;
- (t) Use any data mining, robots, or similar data gathering and extraction methods in connection with the Services or Materials;
- (u) Host, on a subscription basis or otherwise, the Services without Adobe's authorization, including any related application, (i) to permit a third party to use the Services to create, transmit, or protect any content, or (ii) to conduct conferences or online meeting services for a third party;
- (v) Defraud, defame, or otherwise violate the legal rights (such as rights of privacy and publicity) of others; or
- (w) Collect or store data about other users in connection with the prohibited conduct and activities set forth in this Section 8.2.

9. Your Material.

9.1 Storage. Adobe may provide online storage for Your Material, subject to Section 9.2 below and any Additional Terms that may further define the scope of such storage. Unless otherwise stated in Additional Terms or a separate written agreement between you and Adobe, Adobe has (a) no obligation to store Your Material and (b) no responsibility or liability for the deletion or accuracy of any Materials, including Your Material, the failure to store, transmit, or receive transmission of Materials, or the security, privacy, storage, or transmission of other communications originating with or involving use of the Services.

9.2 You agree that Adobe retains the right to create reasonable limits on the use of the Materials, including Your Material, such as limits on file size, storage space, processing capacity, and similar limits described in the web pages accompanying the Services and as otherwise determined by Adobe

in its sole discretion. Adobe may require you to delete Your Material until you are within the storage space limit associated with your account.

9.3 You agree that you, not Adobe, are entirely responsible for all of Your Material that you Share, whether publicly posted or privately transmitted. You assume all risks associated with use of Your Material, including any reliance on its accuracy, completeness, or usefulness.

9.4 Settings Related to Use and Access of Your Material.

(a) Certain Services may enable you to specify the level at which such Services restrict access to Your Material. You are solely responsible for applying the appropriate level of access to Your Material. If you do not choose the access level to apply to Your Material, the system may default to its most permissive setting.

(b) Adobe may allow other Users to comment on Your Shared Material unless you disable the commenting feature.

(c) Adobe may allow you to import your contacts to the Services. For example, Adobe may provide tools to help you upload email addresses of your contacts. If you provide Adobe your password to retrieve those contacts, Adobe will not store the password after you have uploaded the contact information. In addition, Adobe will not store these email addresses you have uploaded once you have found and connected with your friends.

9.5 Licenses to Your Material. Adobe requires certain licenses from you with respect to Your Shared Material in order to operate and enable the Services. Accordingly, you grant the licenses to Your Shared Material as follows:

(a) For Your Shared Material that's Shared in a public forum (such as discussion boards or public galleries that may be browsed by anyone with an internet connection, etc.), you grant Adobe a worldwide, royalty-free, non-exclusive, transferable, and sublicensable license to adapt, display, distribute, modify, perform, publish, reproduce, translate, and use Your Shared Material for the purpose of operating and improving the Services and enabling your use of the Services. You may revoke the license and terminate Adobe's rights at any time by making it no longer Shared.

(b) For Your Shared Material that's Shared in a public forum or shared privately with other Users of your choosing, you grant other Users a worldwide, royalty-free, non-exclusive, transferrable, and sublicensable license to display, distribute, perform, and reproduce Your Material, subject to Section 10 of these Terms. If you join or participate in a group that allows for sharing of Your Material within the group (such as a "group album" or shared workspace), then you also grant the Users within the group a license to adapt and modify Your Material that you have decided to share with such group. If you do not want to grant other Users these rights, then don't Share Your Material with other Users.

(c) For Your Material that is shared privately with other Users of your choosing, you grant Adobe a worldwide, royalty-free, nonexclusive, transferrable, and sublicensable, license to distribute, modify, publish, reproduce, translate, and use Your Material for the purpose of operating and improving the Services and enabling your use of the Services. You may revoke this license and terminate Adobe's rights at any time by removing Your Material from the Service; provided that you agree that Adobe may retain and use copies of Your Material for archival or "backup" purposes and pursuant to Section 15 (Investigations).

(d) You may also grant Adobe specific or different license pursuant to the Additional Terms.

9.6 You acknowledge that the Services are automated (e.g., Your Material is uploaded using software tools) and that Adobe personnel will not access, view, or listen to any of Your Material, except as reasonably necessary to perform the Services, including but not limited to the following:

(a) respond to support requests;

(b) detect, prevent, or otherwise address fraud, security, or technical issues; (c) as deemed necessary or advisable by Adobe in good faith to conform to legal requirements or comply with legal process;
or (d) enforce these Terms, including investigation of potential violations hereof, as further described in Section 15 (Investigations).

9.7 You acknowledge and agree that although Adobe endeavors to provide security measures to protect Your Material (including Your Shared Material that you Shared privately), Adobe is not liable for any damages resulting for the disclosure of Your Material.

10. Shared Material.

10.1 **License to Shared Material.** Adobe grants you a worldwide, royalty-free, and non-exclusive license to distribute, display, download, perform, and reproduce the Material, subject to the restrictions stated in this Section 10. With respect to Shared Material Shared in a group allowing for content sharing, Adobe also grants you the license to adapt and modify such Shared Material. The license granted in this Section 10.1

is further limited to your personal and internal use purposes only.

10.2 It is your sole responsibility to determine what limitations, if any, are placed on your Shared Material. Adobe cannot and does not monitor or control what others do with the Shared Material, nor can Adobe prevent them from adding to, modifying, or adapting the Shared Material.

10.3 You agree that Adobe has no liability of any kind should other Users use, modify, destroy, corrupt, copy, or distribute your Shared Material in violation of the limitations that you may impose on its use.

10.4 Shared Material may include personal information (such as email addresses) to facilitate your ability to share Your Material. It is your sole responsibility for any and all personal information that you or other Users used and submitted in connection with the Services. You shall comply with all data protection and privacy laws and rules applicable to the personal information of other Users.

10.5 The Services may allow you to comment on Shared Material. Comments are not anonymous and may be viewed by other Users. Your comments may be deleted by you, other Users, or Adobe.

10.6 If you are invited by a user of the Service to participate in shared digital content editing or viewing, and you do not wish to receive email from such User or do not wish to participate, you are required to contact the person who invited you to update, correct, or delete the information they provided about you.

10.7 In general, even though we might delete an account you hold with us in these types of shared editing or viewing areas, we may continue to retain information regarding your past actions with respect to content reviews or sharing initiated by others.

10.8 Upon removal of Your Material from the Service or upon making your Shared Material no longer shared, Adobe shall have a reasonable time to cease use, distribution, and/or display of Your Material. However, you acknowledge and agree that Adobe shall have the right but not the obligation to keep archived or "backup" copies of Your Material or use Your Material pursuant to Section 15 (Investigations).

11. Use of Software.

11.1 Software made available via the Services or through third-party marketplaces or stores is governed by the terms of the applicable Additional Terms or the license agreement referenced in the Software. If there is any conflict between these Terms and the license agreement provided with such Software, then the license agreement shall take precedence in relation to that Software. If the Software is a pre-release version, then you are not permitted to use or otherwise rely on the Software for any commercial or production purposes, notwithstanding anything to the contrary included within an accompanying license agreement.

11.2 Adobe may provide mobile and tablet applications through third parties that interact with the Service and Adobe products. You are responsible for obtaining and maintaining any equipment or ancillary services needed to access mobile and tablet applications and you are responsible for all applicable taxes and fees incurred while accessing such applications (such as fees from your mobile carrier, overage charges, etc.)

11.3 If no license agreement accompanies the Software that is available for download, the download and use of such Software will be governed by the terms of this Section 11.3. Adobe grants you a personal, worldwide, revocable, limited, non-transferable, nonsublicensable, non-assignable, nonexclusive license to use the Software in the manner permitted by the Terms. For clarification, you shall not distribute, lease, rent, sell, or sublicense the Software. You agree that you will not decompile, reverse engineer, or otherwise attempt to discover the source code of the Software. Notwithstanding the foregoing, decompiling the Software is permitted to the extent the laws of the jurisdiction where you are located give you the right to do so to obtain information necessary to render the Software interoperable with other software, provided, however, that you must first request the information from Adobe and Adobe may, in its discretion, either provide such information to you or impose reasonable conditions, including reasonable fees, on use of the Software to ensure that Adobe's Intellectual Property Rights in the Software are protected. You may not assign (or grant a sublicense of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software. For clarity, your use of the Software is also subject to the disclaimers and limitations in Sections 13 and 14 below and your compliance with the export control provisions of Section 22.

11.4 The Software may automatically download and install updates from Adobe. These updates are designed to improve, enhance and further develop the Services and may take the form of bug fixes, enhanced functions, new Software modules, and completely new versions. You agree to receive such updates (and permit Adobe to deliver these to you with or without your knowledge) as part of your use of the Services.

12. Your Warranty, Indemnification Obligation, and Waiver.

12.1 You represent and warrant that: (a) you own the Intellectual Property Rights, or have obtained all necessary license(s) and permission(s), to use Your Material in keeping with your use in connection with the Services or as otherwise permitted by the Terms; (b) you have the rights necessary to grant the license and sublicenses described in the Terms; (c) you have received consent from any and all persons depicted in Your Material to use Your Material as set forth in the Terms, including distribution, public display, public performance, and reproduction of Your Material; and (d) Your Material does not violate or infringe any intellectual property right or other proprietary right, including right of publicity or privacy, of any person, company or entity, or other third party.

12.2 You agree to indemnify and hold Adobe and its subsidiaries, affiliates, officers, agents, employees, co-branders or other partners, and licensors harmless from any claim or demand, including reasonable attorneys' fees, due to or arising out of Your Material, your use of the Services or Materials, your connection to the Services or Materials, your use and access of personal information of other Users, the actions of any member of your group, your access to or use of Sites or the Linked Sites and your connections therewith, any claim that Your Material caused damage to someone else, any dealings

between you and anyone else advertising or promoting via the Services or Materials, your violation of the Terms, or your violation of any rights of another, including any Intellectual Property Rights.

12.3 You acknowledge and agree that by accessing or using the Services or Materials, you may be exposed to Materials (including Shared Group Material) from others that you may consider offensive, indecent, or otherwise objectionable, and agree to accept that risk.

13. DISCLAIMER OF WARRANTIES.

YOU EXPRESSLY UNDERSTAND AND AGREE THAT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW:

13.1 THE SITE, SERVICES, AND MATERIALS ARE PROVIDED BY ADOBE "AS IS," WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, QUIET ENJOYMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE FOREGOING, ADOBE AND ITS LICENSORS MAKE NO WARRANTY THAT (a) THE SITE, SERVICES OR MATERIALS WILL MEET YOUR REQUIREMENTS OR WILL BE CONSTANTLY AVAILABLE, UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE; (b) THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SITE, SERVICES, OR MATERIALS WILL BE EFFECTIVE, ACCURATE, OR RELIABLE; (c) THE QUALITY OF THE SITE, SERVICES, OR MATERIALS WILL MEET YOUR EXPECTATIONS; OR THAT (d) ANY ERRORS OR DEFECTS IN THE SITE, SERVICES, OR MATERIALS WILL BE CORRECTED. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM ADOBE OR THROUGH OR FROM USE OF THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

13.2 ADOBE SPECIFICALLY DISCLAIMS ANY LIABILITY WITH REGARD TO ANY ACTIONS RESULTING FROM YOUR USE OF OR PARTICIPATION IN ANY SERVICES AND YOUR USE OF MATERIALS. ANY MATERIAL DOWNLOADED, MADE AVAILABLE, OR OTHERWISE OBTAINED THROUGH USE OF THE SERVICES IS ACCESSED AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL. ADOBE ASSUMES NO LIABILITY FOR ANY COMPUTER VIRUS OR SIMILAR CODE THAT IS DOWNLOADED TO YOUR COMPUTER FROM ANY OF THE SERVICES.

13.3 ADOBE DOES NOT CONTROL, ENDORSE, OR ACCEPT RESPONSIBILITY FOR ANY MATERIALS OR SERVICES OFFERED BY THIRD PARTIES ACCESSIBLE THROUGH LINKED SITES. ADOBE MAKES NO REPRESENTATIONS OR WARRANTIES WHATSOEVER ABOUT, AND SHALL NOT BE LIABLE FOR, ANY SUCH THIRD PARTIES, THEIR MATERIALS OR SERVICES. ANY DEALINGS THAT YOU MAY HAVE WITH SUCH THIRD PARTIES ARE AT YOUR OWN RISK.

13.4 MANAGERS, HOSTS, PARTICIPANTS, MODERATORS, AND OTHER THIRD PARTIES ARE NOT AUTHORIZED ADOBE SPOKESPERSONS, AND THEIR VIEWS DO NOT NECESSARILY REFLECT THOSE OF ADOBE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ADOBE WILL HAVE NO LIABILITY RELATED TO USER MATERIAL ARISING UNDER INTELLECTUAL PROPERTY RIGHTS, LIBEL, PRIVACY, PUBLICITY, OBSCENITY, OR OTHER LAWS. ADOBE ALSO DISCLAIMS ALL LIABILITY WITH RESPECT TO THE USE, MISUSE, LOSS, MODIFICATION, OR UNAVAILABILITY OF ANY USER MATERIAL.

13.5 ADOBE WILL NOT BE LIABLE FOR ANY LOSS THAT YOU MAY INCUR AS A RESULT OF SOMEONE ELSE USING YOUR PASSWORD OR ACCOUNT OR ACCOUNT INFORMATION IN CONNECTION WITH THE SITE OR ANY SERVICES OR MATERIALS, EITHER WITH OR WITHOUT YOUR KNOWLEDGE.

13.6 SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, THE LIMITATION OR EXCLUSION OF IMPLIED WARRANTIES, OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

14. Limitation of Liability.

14.1 IN NO EVENT SHALL ADOBE, ITS OFFICERS, DIRECTORS, EMPLOYEES, PARTNERS, LICENSORS, OR SUPPLIERS BE LIABLE TO YOU OR ANYONE ELSE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES WHATSOEVER, INCLUDING THOSE RESULTING FROM LOSS OF USE, DATA, OR PROFITS, WHETHER OR NOT FORESEEABLE OR IF ADOBE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR BASED ON ANY THEORY OF LIABILITY, INCLUDING BREACH OF CONTRACT OR WARRANTY, NEGLIGENCE OR OTHER TORTIOUS ACTION, OR ANY OTHER CLAIM ARISING OUT OF OR IN CONNECTION WITH YOUR USE OF OR ACCESS TO THE SITE, SERVICES OR MATERIALS. NOTHING IN THE TERMS SHALL LIMIT OR EXCLUDE ADOBE'S LIABILITY FOR GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT OF ADOBE OR ITS EMPLOYEES, OR FOR DEATH OR PERSONAL INJURY.

14.2 ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS AFFILIATES, LICENSORS, AND SUPPLIERS UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO US \$100 OR THE AGGREGATE AMOUNT PAID BY YOU FOR ACCESS TO THE SERVICE DURING THE THREE-MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY, WHICHEVER IS LARGER. THIS LIMITATION WILL APPLY EVEN IF ADOBE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

14.3 THE LIMITATIONS AND EXCLUSIONS IN THIS SECTION 14 APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION. SOME JURISDICTIONS PROHIBIT THE EXCLUSION OR LIMITATION OF LIABILITY FOR INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES. ACCORDINGLY, THE LIMITATIONS AND EXCLUSIONS SET FORTH ABOVE MAY NOT APPLY TO YOU.

15. Investigations.

15.1 Adobe, in its sole discretion, may (but has no obligation to) monitor or review the Services and Materials at any time. Without limiting the foregoing, Adobe shall have the right, in its sole discretion, to remove any of Your Material for any reason (or no reason), including if it violates the Terms or any Law.

15.2 Although Adobe does not generally monitor User activity occurring in connection with the Services or Materials, if Adobe becomes aware of any possible violations by you of any provision of the Terms, Adobe reserves the right to investigate such violations, and Adobe may, at its sole discretion, immediately terminate your rights hereunder, including your right to use the Services or Materials, or change, alter, or remove Your Material or Account Information, in whole or in part, without prior notice to you. If, as a result of such investigation, Adobe believes that criminal activity has occurred, Adobe reserves the right to refer the matter to, and to cooperate with, any and all applicable law enforcement authorities. Except to the extent prohibited by applicable Law, Adobe is entitled to retain and/or disclose any information or Materials, including Your Material or Account Information (or elements thereof), in Adobe's possession in connection with your use of the Services to (a) comply with applicable Law, legal process, or governmental request; (b) enforce the Terms; (c) respond to any claims that Your Material violates the Terms or rights of third parties; (d) respond to your requests for customer services; or (e) protect the rights, property or personal safety of Adobe, its Users, or third parties, including the public at large, as Adobe in its sole discretion believes to be necessary or appropriate.

16. Feedback.

You have no obligation to provide Adobe with ideas, suggestions or proposals ("Feedback"). However, if you submit Feedback to Adobe, we may use it for any purpose without compensation to you.

17. Notification of Copyright Infringement.

17.1 Adobe respects the Intellectual Property Rights of others and expects its Users to do the same. Adobe will respond to clear notices of copyright infringement consistent with the Digital Millennium Copyright Act, Title 17, United States Code, Section 512(c) (2) ("DMCA") and its response to such notices may include removing or disabling access to the allegedly infringing Materials, terminating the accounts of repeat infringers, and/or making good-faith attempts to contact the User who posted the Material(s) at issue so that he may, where appropriate, make a counter-notification.

17.2 If you believe that your work has been used or copied in a way that constitutes copyright infringement and such infringement is hosted on the Services, on websites linked to or from the Services, or in connection with the Services or Materials, please provide, pursuant to the DMCA, written notification via regular mail or via fax (not via email or phone) of claimed copyright infringement to Adobe's Copyright Agent (contact information below), which must contain all of the following elements: (a) A physical or electronic signature of the person authorized to act on behalf of the owner of the copyright interest that is alleged to have been infringed; (b) A description of the copyrighted work(s) that you claim have been infringed and identification of what Material in such work(s) is claimed to be infringing and which you request to be removed or access to which is to be disabled; (c) A description of where the Material that you claim is infringing is located on the Services; (d) Information sufficient to permit Adobe to contact you, such as your physical address, telephone number, and email address; (e) A statement by you that you have a good faith belief that the use of the Material identified in your notice in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (f) A statement by you that the information in your notice is accurate and, under penalty of perjury, that you are the copyright owner or are authorized to act on the copyright owner's behalf. Before you file such a notification, please carefully consider whether or not the use of copyrighted material at issue is protected by the "fair use" doctrine, as you could be liable for costs and attorneys' fees should you file a takedown notice where there is no infringing use. If you are unsure whether a use of your copyrighted material constitutes infringement, please contact an attorney. In addition, you may wish to consult publicly available reference materials such as those found at www.chillingeffects.org.

17.3 If you believe access to your Material was disabled or removed by Adobe as a result of an improper copyright infringement notice, please provide, pursuant to the DMCA, written notification via regular mail or via fax (not via email or phone) to Adobe's Copyright Agent (contact information below), which must contain all of the following elements: (a) A physical or electronic signature of the subscriber; (b) Identification of the material that was removed from the Services and the location of the Service on which the material appeared before it was removed; (c) A statement under penalty of perjury that you have a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled; (d) Information sufficient to permit Adobe to contact you, such as your physical address, telephone number, and email address; and (e) A statement that you consent to jurisdiction of the Federal District court for the district where you reside (or of Santa Clara County, California if you reside outside of the United States) and that you will accept service of process from the person who provided notification under DMCA subsection (c)(1)(C) or an agent of such person. Before you file such a counter-notification, please carefully consider whether or not the use of the copyrighted material at issue is infringing, as you could be liable for costs and attorneys' fees in the event that a court determines your counter-notification misrepresented that the material was removed by mistake. If you are unsure whether use of the material at issue constitutes infringement, please contact an attorney. In addition, you may wish to consult publicly available reference materials such as those found at www.chillingeffects.org.

17.4 Adobe's Copyright Agent for notice of claims of copyright infringement can be reached as follows:

By mail:

Copyright Agent

Adobe Systems Incorporated

601 Townsend Street

San Francisco, CA 94103

By fax: (415) 723-7869

By email: copyright@adobe.com

By telephone: (408) 536-4030

The Copyright Agent will not remove Material from the Services in response to phone or email notifications regarding allegedly infringing Material, since a valid DMCA notice must be signed, under penalty of perjury, by the copyright owner or by a person authorized to act on his or her behalf. Please submit such notifications by fax or ordinary mail only and as further described by this Section. The Copyright Agent should be contacted only if you believe that your work has been used or copied in a way that constitutes copyright infringement and that such infringement is occurring on the Services or on sites linked to or from the Services, or in connection with the Services or Materials. All other inquiries directed to the Copyright Agent will not be responded to.

18. Advertising and Your Material.

You agree that Adobe may display advertisements adjacent to Your Material, and you agree that you are not entitled to any compensation. The manner, mode, and extent of advertising or other revenue generating models pursued by Adobe on or in conjunction with the Services and/or Your Material are subject to change without specific notice to you.

19. Links to Other Sites.

The Services and Materials may include links that will take you websites or services not operated by Adobe. Whether the link was provided by Adobe as a courtesy, or whether it was posted by a User, Adobe has no control over non-Adobe websites or services. You agree that we are not responsible for the availability or contents of any website or service we do not operate.

20. Termination.

20.1 Termination by You.

(a) As either an individual user or a group administrator for a Service, You may stop using the Service at any time. You may terminate Adobe's right to distribute, publicly perform, and publicly display Your Shared Material by making it no longer Shared. You may terminate the remainder of Adobe's rights by removing Your Material from the Service, either by deleting it manually, or by contacting Customer Care to have your subscription cancelled, if applicable, and content deleted. To terminate your Service account contact Support at http://www.adobe.com/go/support_contact. Any fees paid by you prior to your termination are not refundable. Termination of your account shall not relieve you of any obligation to pay any accrued fees or charges.

(b) As a group administrator for a Service, you may terminate an individual User's access to a Service at any time.

20.2 Termination by Adobe. Subject to Additional Terms for certain Services and any associated subscription terms and conditions, Adobe may at any time terminate our agreement with you (or any individual Additional Terms) if: (a) You have breached any provision of the Terms (or have acted in a manner that clearly shows you do not intend to, or are unable to, comply with the Terms); (b) Adobe is required to do so by Law (for example, where the provision of the Services or Materials to you is, or becomes, unlawful);

(c) The provision of the Services to you by Adobe is, in Adobe's opinion, no longer commercially viable; (d) Adobe has elected to discontinue the Services or Materials (or any part thereof); or (e) There has been an extended period of inactivity in your account.

20.3 Termination or Suspension of Services. Adobe may also terminate or suspend all or a portion of your account and/or access to the Services for any reason (subject to Additional Terms for certain Services). Except as may be set forth in any Additional Terms applicable to a particular Service, termination of your account may include: (a) removal of access to all offerings within the Services; (b) deletion of Your Material and Account Information, including your personal information, log-in ID and password, and all related information, files, and Materials associated with or inside your account (or any part thereof); and (c) barring of further use of the Services.

20.4 You agree that all terminations for cause shall be made in Adobe's sole discretion and that Adobe shall not be liable to you or any third party for any termination of your account (and accompanying deletion of your Account Information), or access to the Services and Materials, including Your Material.

20.5 Upon expiration or termination of the Terms, you shall promptly discontinue use of the Services and Materials. However, any perpetual licenses you have granted, any of your indemnification obligations hereunder, any of Adobe's disclaimers or limitations of damages or liabilities hereunder, and Sections 8-10, 12-16, 18, 20, 23, and 24 will survive any termination or expiration of the Terms.

20.6 Upon termination of your use of the Service by you or by Adobe for any other reason other than for cause, Adobe will make reasonable effort to notify you at least thirty (30) days prior to termination, at the email address you provide Adobe as part of your registration, with instructions on how to retrieve Your Material prior to such termination.

20.7 If your group administrator terminates your access to a Service, then you may no longer be able to access Shared Material that you or other users of the group have posted to a shared workgroup or shared workspace within that Service. You may, however, still access the Materials stored on your account, subject to Section 9.2 above.

20.8 Except as otherwise stated in any Additional Terms and applicable subscription terms, in the event of termination by Adobe for reasons other than breach of these Terms, Adobe will provide notice pursuant to the General Terms and will provide you with a pro rata refund for the prepaid and unused portion of the Service.

21. International Users.

21.1 The Services can be accessed from countries around the world and may contain references to Services and Materials that are not available in your country. These references do not imply that Adobe intends to announce such Services or Materials in your country.

21.2 These Services are controlled, operated, and administered by Adobe Systems Incorporated from its offices in the United States of America. Adobe makes no representation that the Services or Materials are appropriate or available for use outside of the United States. Adobe reserves the right to block access to the Services or Materials by certain international users. If you access the Services from a location outside the United States, then you are responsible for compliance with all local Laws.

22. Export Control Laws.

You acknowledge that the Services, Software, and Materials are subject to the U.S. Export Administration Regulations and other export laws, restrictions, and regulations (collectively, the "Export Laws") and that you will comply with the Export Laws. You will not ship, transfer, export, or re-export the Software or Materials, directly or indirectly, to: (a) any countries that are subject to U.S. export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan, and Syria) (each, an "Embargoed Country"),

(b) any end user whom you know or have reason to know will utilize them in the design, development, or production of nuclear, chemical, or biological weapons, or rocket systems, space launch vehicles, and sounding rockets, or unmanned air vehicle systems (each, a "Prohibited Use"), or (c) any end user who has been prohibited from participating in the U.S. export transactions by any federal agency of the U.S. government (each, a "Sanctioned Party"). In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export, or use the Services, Software, or Materials. You represent and warrant that (i) you are not a citizen of, or located within, an Embargoed Country, (ii) you will not use the Services, Software, or Materials for a Prohibited Use, and (iii) you are not a Sanctioned Party. All rights to use the Services, Software, and Materials are granted on condition that such rights are forfeited if Customer fails to comply with the terms of this agreement. If Adobe has knowledge that a violation has occurred, Adobe may be prohibited from providing maintenance and support for the Services, Software, or Materials.

23. Resolution of Disputes.

23.1 **Venue.** You agree that any claim or dispute you may have against Adobe must be resolved by a court located in Santa Clara County, California, United States of America except as otherwise agreed by the parties. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California, United States of America when the laws of California apply, and the courts of Dublin, Ireland, when the laws of Ireland applies, for the purpose of litigating such claims or disputes. The parties specifically disclaim the U.N. Convention on Contracts for the International Sale of Goods.

23.2 **All claims you bring against Adobe must be resolved in accordance with this section.** All claims filed or brought contrary to this section shall be considered improperly filed. Should you file a claim contrary to this section, Adobe may recover attorneys' fees and costs up to U.S. \$1,000, provided that Adobe has notified you in writing of the improperly filed claim and you have failed to properly withdraw the claim.

23.3 **Notwithstanding the foregoing, in the event of your or others' unauthorized access to or use of the Services or Materials in violation of the Terms you agree that Adobe shall be entitled to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.**

24. Miscellaneous.

24.1 **English Version.** The English version of this agreement will be the version used when interpreting or construing this agreement.

24.2 **Notice to Adobe.** Any notice provided to Adobe pursuant to the Terms should be sent to 345 Park Avenue, San Jose, California 95110-2704, Attention: General Counsel.

24.3 **Notice to You.** Adobe may provide you with notices, including those regarding changes to the Terms, by email, regular mail, text message, postings on or within the Services, or other reasonable means now known or hereafter developed.

24.4 **Entire Agreement.** The Terms constitute the entire agreement between Adobe and you with respect to your access to or use of the Services and Materials and supersede any prior agreements between you and Adobe on such subject matter.

24.5 **Non-Assignment.** You may not assign or otherwise transfer the Terms, or any right granted hereunder, without Adobe's written consent. Adobe's rights under the Terms are transferable by Adobe.

24.6 **Severability.** If for any reason a court of competent jurisdiction finds any provision of the Terms, or portion thereof, to be unenforceable, that provision shall be enforced to the maximum extent permissible

so as to affect the intent of the parties as reflected by that provision, and the remainder of the Terms shall continue in full force and effect.

24.7 Waiver. Any failure by Adobe to enforce or exercise any provision of the Terms, or any related right, shall not constitute a waiver of that provision or right.

24.8 Report Abuse. Please report any violations of the Terms via the report abuse mechanism offered in conjunction with the specific Service in which the alleged violation occurs.

24.9 You are solely responsible for your familiarity and compliance with any laws that may prohibit you from participating in or using any part of the Services.

Adobe_General_Terms_of_Use-en_US-20121016_1205

Adobe Systems Incorporated: 345 Park Avenue, San Jose, California 95110-2704

Adobe Systems Software Ireland Limited: 4-6 Riverwalk, City West Business Campus, Saggart, Dublin 24

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT OFFICE 2010 DESKTOP APPLICATION SOFTWARE

Below are three separate sets of license terms. Only one set applies to you. To determine which license terms apply to you check the license designation printed either on your product key, near the product name on your Certificate of Authenticity, or on the download page if you obtained your product key online. If your designation is FPP, then the Retail License Terms below apply to you. If your designation is OEM, then the OEM License Terms below apply to you. If your designation is Product Key Card or PKC, then the Product Key Card License Terms below apply to you. If you need assistance finding your license type, please go to: www.microsoft.com/office/eula to determine which license you have.

1. RETAIL LICENSE TERMS.

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. Printed-paper license terms, which may come with the software, may replace or modify an on-screen license terms. These terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE. INSTEAD, RETURN IT TO THE RETAILER FOR A REFUND OR CREDIT. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft's refund policies. See www.microsoft.com/worldwide. In the United States and Canada, call (800) MICROSOFT or see www.microsoft.com/info/nareturns.htm. AS DESCRIBED BELOW, USING THE SOFTWARE ALSO OPERATES AS YOUR CONSENT TO THE TRANSMISSION OF CERTAIN COMPUTER INFORMATION DURING ACTIVATION, VALIDATION AND FOR INTERNET-BASED SERVICES.

IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW FOR EACH LICENSE YOU ACQUIRE.

1. OVERVIEW. The software is licensed on a per copy per device basis. A hardware partition or blade is considered to be a separate device.

2. INSTALLATION AND USE RIGHTS.

- a. One Copy per Device. You may install one copy of the software on one device. That device is the "licensed device."
- b. Licensed Device. You may only use one copy of the software on the licensed device at a time.
- c. Portable Device. You may install another copy of the software on a portable device for use by the single primary user of the licensed device.

d. Separation of Components. The components of the software are licensed as a single unit. You may not separate the components and install them on different devices.

e. Alternative Versions. The software may include more than one version, such as 32-bit and 64-bit. You may install and use only one version at a time.

3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Multiplexing. Hardware or software you use to

- pool connections,
- reroute information, or
- reduce the number of devices or users that directly access or use the software

(sometimes referred to as "multiplexing" or "pooling"), does not reduce the number of licenses you need.

b. Font Components. While the software is running, you may use its fonts to display and print content. You may only

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to print content.

c. Media Elements and Templates. You may have access to media images, clip art, animations, sounds, music, video clips, templates and other forms of content ("media elements") provided with the software or as part of a service associated with the software. You may copy and use the media elements in projects and documents. You may not (i) sell, license or distribute copies of the media elements by themselves or as a product if the primary value of the product is the media elements; (ii) grant your customers rights to further license or distribute the media elements; (iii) license or distribute for commercial purposes media elements that include the representation of identifiable individuals, governments, logos, trademarks, or emblems or use these types of images in ways that could imply an endorsement or association with your product, entity or activity; or (iv) create obscene or scandalous works using the media elements. For more information, go to www.microsoft.com/permission.

d. Use with Virtualization Technologies. Instead of using the software directly on the licensed device, you may install and use the software within only one virtual (or otherwise emulated) hardware system on the licensed device.

e. Remote Access. The single primary user of the licensed device may access and use the software installed on the licensed device remotely from any other device. You may allow others to access the software to provide you with support services. You do not need additional licenses for this access. No other person may use the software under the same license at the same time for any other purpose.

f. Development Tools. The software may contain Microsoft Visual Studio Tools for Applications or other development tools. You may use any

development tools included in the software only to design, develop, test, use and demonstrate your programs with the software.

g. Language Version Selection. If you are provided with a one-time selection between language versions, without a language pack or LIP, you may use only the one language version you select. If you were not provided with a language selection, the language version will default to the language of your operating system or, if your operating system language is not available, to another available language. If you acquire a language pack or LIP, you may use the additional languages included in the language pack or LIP. A "LIP" is a Language Interface Pack. Language packs and LIPs offer additional language version support of the software. The language packs and LIPs are a part of the software and may not be used separately.

h. Trial and Conversion. Some or all of the software may be licensed on a trial basis. Your rights to use trial software are limited to the trial period. The trial software and length of the trial period are set forth during the activation process. You may have the option to convert your trial rights to subscription or perpetual rights. Conversion options will be presented to you at the expiration of your trial period. After the expiration of any trial period without conversion, most features of the trial software will stop running. At that time you can continue to open, view and print any documents you created with the trial software.

i. Subscription Software. If you licensed the software on a subscription basis, your rights to use the software are limited to the subscription period. You may have the option to extend your subscription or convert to a perpetual license. If you extend your subscription, you may continue using the software until the end of your extended subscription period. See the software activation screens or other accompanying materials for subscription details. After the expiration of your subscription, most features of the software will stop running. At that time you can continue to open, view and print any documents you created with the software.

4. MANDATORY ACTIVATION. Activation associates the use of the software with a specific device. During activation, the software will send information about the software and the device to Microsoft. This information includes the version, the license version, language and product key of the software, the Internet protocol address of the device, and information derived from the hardware configuration of the device. For more information, see www.microsoft.com/piracy/activation.msp. BY USING THE SOFTWARE, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. If properly licensed, you have the right to use the version of the software installed during the installation process up to the time permitted for activation. UNLESS THE SOFTWARE IS ACTIVATED, YOU HAVE NO RIGHT TO USE THE SOFTWARE AFTER THE TIME PERMITTED FOR ACTIVATION. This is to prevent its unlicensed use. YOU ARE NOT PERMITTED TO BYPASS OR CIRCUMVENT ACTIVATION. You can activate the software by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. THE SOFTWARE WILL REMIND YOU TO ACTIVATE IT UNTIL YOU DO.

5. VALIDATION.

a. The software will from time to time request download of the validation feature of the software. Validation verifies that the software has been activated and is properly licensed. A validation check confirming that you are properly licensed permits you to use the software, certain features of the software or to obtain additional benefits. For more information, see www.microsoft.com/genuine/office/WhyValidate.aspx.

b. During or after a validation check, the software may send information about the software, the device and the results of the validation check to Microsoft. This information includes, for example, the version and product key of the software and the Internet protocol address of the licensed device. Microsoft does not use the information to identify or contact you. BY USING THE SOFTWARE, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. For more information about validation and what is sent during or after a validation check, see www.microsoft.com/genuine/office/PrivacyInfo.aspx.

c. If, after a validation check, the software is found to be counterfeit, improperly licensed, or a non-genuine Office product then the functionality or experience of using the software may be affected. For example, Microsoft may

- provide notice that the software is improperly licensed or a non-genuine Office product;
- and you may
- receive reminders to obtain a properly licensed copy of the software; or
- need to follow Microsoft's instructions to be licensed to use the software and reactivate;
- and you may not be able to
- use or continue to use the software or some of the features of the software; or
- obtain certain updates or upgrades from Microsoft.

e. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources, see www.microsoft.com/genuine/downloads/faq.aspx.

6. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

a. Consent for Internet-Based Services. The software features described below and in the Office 2010 Privacy Statement connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. In some cases, you may switch off these features or not use them. For more information about these features, see the Office 2010 Privacy Statement at r.office.microsoft.com/r/rlidOOClientPrivacyStatement14?clid=1033. BY USING THESE FEATURES, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. Microsoft does not use the information to identify or contact you. Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the device

where you installed the software. Microsoft uses this information to make the Internet-based services available to you.

- Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance and help. You may choose not to use these web content features.

- Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists using the Internet, when available.

- SharePoint Workspace. If the software includes Microsoft SharePoint Workspace ("SharePoint Workspace"), SharePoint Workspace will allow you to communicate directly with others over the Internet. If you cannot communicate directly with a contact over the Internet, and your administrator uses Microsoft's public server infrastructure, your communications will be encrypted and sent through Microsoft servers for later delivery. You cannot disable this service if your administrator uses Microsoft's public server infrastructure.

SharePoint Workspace makes some information about your SharePoint Workspace account and device known to your approved contacts. For example, if you:

- add a contact to your contact list,
 - import your user account onto a new device,
 - update the information in your "identity contact", or
 - send a SharePoint Workspace invitation using an URL to reference the invitation file,
- information about you and your devices may be sent to your contacts. If you configure SharePoint Workspace to use Microsoft servers, those servers will collect information about your device and user accounts.

b. Automatic Update. Software with Click-to-Run technology may periodically check with Microsoft for updates and supplements to the software. If found, these updates and supplements might be automatically downloaded and installed on your licensed device.

c. Use of Information. Microsoft may use the device information, error reports, and malware reports to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

d. Misuse of Internet-based Services. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

7. SCOPE OF LICENSE. The software is licensed, not sold. This agreement only gives you some rights to use the features included in the software edition you licensed. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so,

you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- use the software in any way that is against the law;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

8. BACKUP COPY.

a. Media. If you acquired the software on a disc or other media, you may make one backup copy of the media. You may use it only to reinstall the software on the licensed device.

b. Electronic Download. If you acquired and downloaded the software online, you may make one copy of the software on a disc or other media in order to install the software on the licensed device. You may also use it to reinstall the software on the licensed device.

c. Click-to-Run. If you acquired and downloaded software online with Click-to-Run technology, you will not be able to make a copy of the software on a disc or other media. Instead you may download the software online again only to reinstall the software on the licensed device.

9. DOCUMENTATION. Any person that has valid access to your licensed device or internal network may copy and use the documentation for your internal, reference purposes.

10. NOT FOR RESALE SOFTWARE. You may not sell software marked as "NFR" or "Not for Resale."

11. ACADEMIC SOFTWARE. You must be a "Qualified Educational User" to use software marked as "Academic" edition. If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.

12. HOME AND STUDENT SOFTWARE. For software marked "Home and Student" edition, you may install one copy of the software on up to three licensed devices in your household for use by people for whom that is their primary residence. The software may not be used for commercial, non-profit, or revenue-generating activities.

13. MILITARY APPRECIATION SOFTWARE. You must be a "Qualified Military User" to license software marked as "Military Appreciation" edition. To be a Qualified Military User, in the United States of America, you must be an authorized patron of the Armed Services Exchanges in accordance with applicable U.S. Federal statutes and regulations. The software is not licensed for use in any commercial, non-profit, or revenue-generating activities. If the software is marked as "Military Appreciation" edition,

you may only transfer this software in accordance with military exchange service policies and regulations.

14. CANADIAN FORCES SOFTWARE. You must be a "CANEX Authorized Patron" to license software marked as "Canadian Forces" edition. To be a CANEX Authorized Patron, you must be a

- Serving member of the Canadian Forces (CF) or their spouse;
- Member of the Canadian Forces Reserve Force;
- Retired Canadian Forces member or Department of National Defense (DND) civilian employee in receipt of a DND pension;
- Permanent full time or part time Non-Public Fund (NPF) or DND employee or and their spouse;
- CANEX Concessionaire (principals only);
- Qualifying foreign military personnel;
- Retired NPF employee in receipt of an NPF pension;
- Full time employee of Alternative Service Delivery contractors;
- Widow of CF personnel receiving a benefit under the Child Family Services Act, Defence Services Pension Contribution Act, or the Pension Act or the War Veterans Allowance Act;
- Member of the Canadian Corps of Commissionaires when residing or employed on a Base/Wing; or
- Member of the Royal Canadian Mounted Police.

The software is not licensed for use in any commercial, non-profit, or revenue-generating activities. If the software is marked as "Canadian Forces" edition, you may only transfer this software in accordance with Canex retail store service policies and regulations.

15. HOME USE PROGRAM SOFTWARE. You must be a "Home Use Program User" to use software marked as "Home Use Program". To be a Home Use Program User, you must be both:

- an employee of an organization that has a Microsoft Volume License agreement with Software Assurance, and
- the user of a licensed copy of the software, or a product that includes the software, with active Software Assurance.

16. GEOGRAPHIC RESTRICTIONS. If the software is marked as requiring activation in a specific geographic region, then you are only permitted to activate this software in the geographic region indicated on the software packaging. You may not be able to activate the software outside of that region. For further information on geographic restrictions, visit go.microsoft.com/fwlink/?LinkId=141397.

17. UPGRADE OR CONVERSION. To upgrade or convert software, you must first be licensed for the software that is eligible for the upgrade or conversion. Upon upgrade or conversion, this agreement takes the place of the agreement for the software you upgraded or converted from. After you upgrade or convert, you may no longer use the software you upgraded or converted from.

18. PROOF OF LICENSE.

a. Genuine Proof of License. If you acquired the software on a disc or other media, your proof of license is the genuine Microsoft certificate of authenticity label with the accompanying genuine product key and your proof of purchase. If you purchased and downloaded the software online,

your proof of license is the genuine Microsoft product key for the software which you received with your purchase and your proof of purchase from an authorized electronic supplier of genuine Microsoft software. Proof of purchase may be subject to verification by your merchant's records.

b. Upgrade or Conversion License. If you upgrade or convert the software, your proof of license is

- the genuine proof of license for the software you upgraded or converted from; and
- the genuine proof of license for the software you upgraded or converted to.

c. To identify genuine Microsoft software, see www.howtotell.com.

19. REASSIGN TO ANOTHER DEVICE. You may reassign the license to a different device any number of times, but not more than one time every 90 days. If you reassign, that other device becomes the "licensed device." If you retire the licensed device due to hardware failure, you may reassign the license sooner.

20. TRANSFER TO A THIRD PARTY. The first user of the software may make a one-time transfer of the software and this agreement, by transferring the genuine proof of license directly to a third party. The first user must remove the software before transferring it separately from the licensed device. The first user may not retain any copies of the software. Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software. If the software is an upgrade, any transfer must also include all prior versions of the software.

21. EXPORT RESTRICTIONS. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

22. SUPPORT SERVICES. Microsoft provides support services for the software as described at www.support.microsoft.com/common/international.aspx.

23. ENTIRE AGREEMENT. This agreement (including the warranty below), any addendum or amendment included with the software, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

24. APPLICABLE LAW.

a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the software in any other

country, the laws of that country apply.

25. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

26. LIMITATION ON AND EXCLUSION OF DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO THE AMOUNT YOU PAID FOR THE SOFTWARE. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES. This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if

- repair, replacement or a refund for the software does not fully compensate you for any losses; or
- Microsoft knew or should have known about the possibility of the damages.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

LIMITED WARRANTY

A. LIMITED WARRANTY. If you follow the instructions, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

B. TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. THE LIMITED WARRANTY COVERS THE SOFTWARE FOR ONE YEAR AFTER ACQUIRED BY THE FIRST USER. IF YOU RECEIVE SUPPLEMENTS, UPDATES, OR REPLACEMENT SOFTWARE DURING THAT YEAR, THEY WILL BE COVERED FOR THE REMAINDER OF THE WARRANTY OR 30 DAYS, WHICHEVER IS LONGER. If the first user transfers the software, the remainder of the warranty will apply to the recipient. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES, GUARANTEES OR CONDITIONS LAST ONLY DURING THE TERM OF THE LIMITED WARRANTY. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee or condition lasts.

C. EXCLUSIONS FROM WARRANTY. This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond Microsoft's reasonable control.

D. REMEDY FOR BREACH OF WARRANTY. MICROSOFT WILL REPAIR OR REPLACE THE SOFTWARE AT NO CHARGE. IF MICROSOFT CANNOT REPAIR OR REPLACE IT, MICROSOFT WILL REFUND THE AMOUNT SHOWN ON YOUR RECEIPT FOR THE SOFTWARE. IT WILL ALSO REPAIR OR REPLACE SUPPLEMENTS, UPDATES AND REPLACEMENT SOFTWARE AT NO

CHARGE. IF MICROSOFT CANNOT REPAIR OR REPLACE THEM, IT WILL REFUND THE AMOUNT YOU PAID FOR THEM, IF ANY. YOU MUST UNINSTALL THE SOFTWARE AND RETURN ANY MEDIA AND OTHER ASSOCIATED MATERIALS TO MICROSOFT WITH PROOF OF PURCHASE TO OBTAIN A REFUND. THESE ARE YOUR ONLY REMEDIES FOR BREACH OF THE LIMITED WARRANTY.

E. CONSUMER RIGHTS NOT AFFECTED. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS, WHICH THIS AGREEMENT CANNOT CHANGE.

F. WARRANTY PROCEDURES. You need proof of purchase for warranty service.

1. United States and Canada. For warranty service or information about how to obtain a refund for software acquired in the United States and Canada, contact Microsoft at

- (800) MICROSOFT;
- Microsoft Customer Service and Support, One Microsoft Way, Redmond, WA 98052-6399; or
- visit www.microsoft.com/info/nareturns.htm.

2. Europe, Middle East and Africa. If you acquired the software in Europe, the Middle East or Africa, Microsoft Ireland Operations Limited makes this limited warranty. To make a claim under this warranty, you should contact either

- Microsoft Ireland Operations Limited, Customer Care Centre, Atrium Building Block B, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Ireland; or
- the Microsoft affiliate serving your country (see www.microsoft.com/worldwide).

3. Outside United States, Canada, Europe, Middle East and Africa. If you acquired the software outside the United States, Canada, Europe, the Middle East and Africa, contact the Microsoft affiliate serving your country (see www.microsoft.com/worldwide).

G. NO OTHER WARRANTIES. THE LIMITED WARRANTY IS THE ONLY DIRECT WARRANTY FROM MICROSOFT. MICROSOFT GIVES NO OTHER EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. WHERE ALLOWED BY YOUR LOCAL LAWS, MICROSOFT EXCLUDES IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. If your local laws give you any implied warranties, guarantees or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

H. LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. THE LIMITATION ON AND EXCLUSION OF DAMAGES CLAUSE ABOVE APPLIES TO BREACHES OF THIS LIMITED WARRANTY. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE. YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM COUNTRY TO COUNTRY.

2. OEM LICENSE TERMS

These license terms are an agreement between you and

- the device manufacturer that distributes the software with the device; or
- the software installer that distributes the software with the device.

Please read them. They apply to the software that accompanies these license terms, which includes the media on which you received it, if any. Printed-paper license terms, which may come with the software, take the place of any on-screen license terms. These terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those other terms apply.

If you obtain updates or supplements directly from Microsoft, then these terms apply except that Microsoft, and not the manufacturer or installer, licenses those to you.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE. INSTEAD, CONTACT THE MANUFACTURER OR INSTALLER TO DETERMINE ITS RETURN POLICY FOR A REFUND OR CREDIT. AS DESCRIBED BELOW, USING THE SOFTWARE ALSO OPERATES AS YOUR CONSENT TO THE TRANSMISSION OF CERTAIN COMPUTER INFORMATION DURING ACTIVATION, VALIDATION AND FOR INTERNET-BASED SERVICES. IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW FOR EACH LICENSE YOU ACQUIRE.

1. OVERVIEW. The software is licensed on a per copy per device basis. A hardware partition or blade is considered to be a separate device.

2. INSTALLATION AND USE RIGHTS.

a. One Copy per Device. The software license is permanently assigned to the device with which the software is distributed. That device is the "licensed device."

b. Licensed Device. You may only use one copy of the software on the licensed device at a time.

c. Separation of Components. The components of the software are licensed as a single unit. You may not separate the components and install them on different devices.

d. Alternative Versions. The software may include more than one version, such as 32-bit and 64-bit. You may use only one version at one time. If the manufacturer or installer provides you with more than one language version, you may use only one language version at one time.

3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Multiplexing. Hardware or software you use to

- pool connections,
- reroute information, or
- reduce the number of devices or users that directly access or use the software (sometimes referred to as "multiplexing" or "pooling"), does not reduce the number of licenses you need.

b. Font Components. While the software is running, you may use its fonts to display and print content. You may only

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to print content.

c. Media Elements and Templates. You may have access to media images, clip art, animations, sounds, music, video clips, templates and other forms of content ("media elements") provided with the software or as part of a service associated with the software. You may copy and use the media elements in projects and documents. You may not (i) sell, license or distribute copies of the media elements by themselves or as a product if the primary value of the product is the media elements; (ii) grant your customers rights to further license or distribute the media elements; (iii) license or distribute for commercial purposes media elements that include the representation of identifiable individuals, governments, logos, trademarks, or emblems or use these types of images in ways that could imply an endorsement or association with your product, entity or activity; or (iv) create obscene or scandalous works using the media elements. For more information, go to www.microsoft.com/permission.

d. Use with Virtualization Technologies. Instead of using the software directly on the licensed device, you may install and use the software within only one virtual (or otherwise emulated) hardware system on the licensed device.

e. Remote Access. The single primary user of the licensed device may access and use the software installed on the licensed device remotely from any other device. You may allow others to access the software to provide you with support services. You do not need additional licenses for this access. No other person may use the software under the same license at the same time for any other purpose.

f. Development Tools. The software may contain Microsoft Visual Studio Tools for Applications or other development tools. You may use any development tools included in the software only to design, develop, test, use and demonstrate your programs with the software. These license terms apply to your use of the tools.

g. Language Version Selection. If the computer manufacturer provides you with a one-time selection between language versions, you may use only the one language version you select. If you were not provided with a language selection, the language version will default to the language of your operating system or, if your operating system language is not available, to another available language. If the computer manufacturer provides you with a language pack or "LIP", you may use the additional languages included in the language pack or LIP. A "LIP" is a Language Interface Pack. Language packs and LIPs offer additional language version support of the software. The language packs and LIPs are a part of the software and may not be used separately.

h. Trial and Conversion. Some or all of the software may be licensed on a trial basis. Your rights to use trial software are limited to the trial period. The trial software and length of the trial period are set forth during the activation process. You may have the option to convert your trial rights to subscription or perpetual rights. Conversion options will be presented to you at the expiration of your trial period. After the expiration of any trial period without conversion, most features of the trial software will stop running. At that time you can continue to open, view and print any documents you created with the trial software.

i. Subscription Software. If you licensed the software on a subscription basis, your rights to use the software are limited to the subscription period. You may have the option to extend your subscription or convert to a perpetual license. If you extend your subscription, you may continue using the software until the end of your extended subscription period. See the software activation screens or other accompanying materials for subscription details. After the expiration of your subscription, most features of the software will stop running. At that time you can continue to open, view and print any documents you created with the software.

4. MANDATORY ACTIVATION. Activation associates the use of the software with a specific device. During activation, the software will send information about the software and the device to Microsoft. This information includes the version, the license version, language and product key of the software, the Internet protocol address of the device, and information derived from the hardware configuration of the device. For more information, see www.microsoft.com/piracy/activation.msp. BY USING THE SOFTWARE, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. If properly licensed, you have the right to use the version of the software installed during the installation process up to the time permitted for activation. UNLESS THE SOFTWARE IS ACTIVATED, YOU HAVE NO RIGHT TO USE THE SOFTWARE AFTER THE TIME PERMITTED FOR ACTIVATION. This is to prevent its unlicensed use. YOU ARE NOT PERMITTED TO BYPASS OR CIRCUMVENT ACTIVATION. You can activate the software by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. THE SOFTWARE WILL REMIND YOU TO ACTIVATE IT UNTIL YOU DO.

5. VALIDATION.

a. The software will from time to time request download of the validation feature of the software. Validation verifies that the software has been activated and is properly licensed. A validation check confirming that you are properly licensed permits you to use the software, certain features of the software or to obtain additional benefits. For more information, see www.microsoft.com/genuine/office/WhyValidate.aspx.

b. During or after a validation check, the software may send information about the software, the device and the results of the validation check to Microsoft. This information includes, for example, the version and product key of the software and the Internet protocol address of the licensed device. Microsoft does not use the information to identify or contact you. BY USING THE SOFTWARE, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. For more information about validation and what is sent during or after a validation check, see www.microsoft.com/genuine/office/PrivacyInfo.aspx.

c. If, after a validation check, the software is found to be counterfeit, improperly licensed, or a non-genuine Office product then the functionality or experience of using the software may be affected. For example, Microsoft may

- provide notice that the software is improperly licensed or a non-genuine Office product;

and you may

- receive reminders to obtain a properly licensed copy of the software; or
- need to follow Microsoft's instructions to be licensed to use the software and reactivate;

and you may not be able to

- use or continue to use the software or some of the features of the software; or
- obtain certain updates or upgrades from Microsoft.

d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources, see www.microsoft.com/genuine/downloads/faq.aspx.

6. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

a. Consent for Internet-Based Services. The software features described below and in the Office 2010 Privacy Statement connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. In some cases, you may switch off these features or not use them. For more information about these features, see the Office 2010 Privacy Statement at r.office.microsoft.com/r/rliid00ClientPrivacyStatement14?clid=1033. BY USING THESE FEATURES, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. Microsoft does not use the information to identify or contact you.

Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the device where you installed the software. Microsoft uses this information to make the Internet-based services available to you.

- Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance and help. You may choose not to use these web content features.

- Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists using the Internet, when available.

- SharePoint Workspace. If the software includes Microsoft SharePoint Workspace ("SharePoint Workspace"), SharePoint Workspace will allow you to communicate directly with others over the Internet. If you cannot communicate directly with a contact over the Internet, and your administrator uses Microsoft's public server infrastructure, your communications will be encrypted and sent through Microsoft servers for later delivery. You cannot disable this service if your administrator uses Microsoft's public server infrastructure.

SharePoint Workspace makes some information about your SharePoint Workspace account and device known to your approved contacts. For example, if you:

- add a contact to your contact list,

- import your user account onto a new device,
- update the information in your "identity contact", or
- send a SharePoint Workspace invitation using an URL to reference the invitation file,

information about you and your devices may be sent to your contacts. If you configure SharePoint Workspace to use Microsoft servers, those servers will collect information about your device and user accounts.

b. Automatic Update. Software with Click-to-Run technology may periodically check with Microsoft for updates and supplements to the software. If found, these updates and supplements might be automatically downloaded and installed on your licensed device.

c. Use of Information. Microsoft may use the device information, error reports, and malware reports to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

d. Misuse of Internet-based Services. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

7. SCOPE OF LICENSE. The software is licensed, not sold. This agreement only gives you some rights to use the features included in the software edition you licensed. The manufacturer or installer and Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. You may not

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- use components of the software to run applications not running on the software;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- use the software in any way that is against the law;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

8. BACKUP COPY. You may make one backup copy of the software media. You may use it only to reinstall the software on the licensed device.

9. DOCUMENTATION. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

10. NOT FOR RESALE SOFTWARE. You may not sell software marked as "NFR" or "Not for Resale."

11. HOME AND STUDENT SOFTWARE. For software marked "Home and Student" edition, you may not use the software for commercial, non-profit, or revenue-generating activities.

12. GEOGRAPHIC RESTRICTIONS. If the software is marked as requiring activation in a specific geographic region, then you are only permitted to activate this software in the geographic region indicated on the software or computer packaging. You may not be able to activate the software outside of that region. For further information on geographic restrictions, visit go.microsoft.com/fwlink/?LinkId=141397.

13. UPGRADE OR CONVERSION. To upgrade or convert software, you must first be licensed for the software that is eligible for the upgrade or conversion. Upon upgrade or conversion, this agreement takes the place of the agreement for the software you upgraded or converted from. After you upgrade or convert, you may no longer use the software you upgraded or converted from.

14. PROOF OF LICENSE.

a. Genuine Proof of License. If you acquired the software on a device, or on a disc or other media, a genuine Microsoft Certificate of Authenticity label with a genuine copy of the software identifies licensed software. To be valid, this label must be affixed to the device or appear on the manufacturer's or installer's packaging. If you receive the label separately, it is invalid. You should keep label on the device or the packaging that has the label on it to prove that you are licensed to use the software. If the device comes with more than one genuine Certificate of Authenticity label, you may use each version for the software identified on those labels.

b. To identify genuine Microsoft software, see www.howtotell.com.

15. TRANSFER TO A THIRD PARTY. You may transfer the software directly to a third party only with the licensed device, the Certificate of Authenticity label, and this agreement. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. You may not retain any copies.

16. EXPORT RESTRICTIONS. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

17. SUPPORT SERVICES. For the software generally, contact the manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft provides support as described at www.support.microsoft.com/common/international.aspx. If you are using software that is not properly licensed, you will not be entitled to receive support services.

18. ENTIRE AGREEMENT. This agreement (including the warranty below), additional terms (including any printed-paper license terms that accompany the software and may modify or replace some or all of these terms), and the

terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

19. APPLICABLE LAW.

a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the software in any other country, the laws of that country apply.

20. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

21. LIMITATION ON AND EXCLUSION OF DAMAGES. EXCEPT FOR ANY REFUND THE MANUFACTURER OR INSTALLER MAY PROVIDE, YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.
- It also applies even if
- repair, replacement or a refund for the software does not fully compensate you for any losses; or
- the manufacturer, installer, or Microsoft knew or should have known about the possibility of the damages.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

LIMITED WARRANTY

A. LIMITED WARRANTY. If you follow the instructions and the software is properly licensed, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

B. TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. THE LIMITED WARRANTY COVERS THE SOFTWARE FOR 90 DAYS AFTER ACQUIRED BY THE FIRST USER. IF YOU RECEIVE SUPPLEMENTS, UPDATES, OR REPLACEMENT SOFTWARE DURING THOSE 90 DAYS, THEY WILL BE COVERED FOR THE REMAINDER OF THE WARRANTY OR 30 DAYS, WHICHEVER IS LONGER. If you transfer the software, the remainder of the warranty will apply to the recipient.

TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES, GUARANTEES OR CONDITIONS LAST ONLY DURING THE TERM OF THE LIMITED WARRANTY. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee or condition lasts.

C. EXCLUSIONS FROM WARRANTY. This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond the reasonable control of the manufacturer or installer, or Microsoft.

D. REMEDY FOR BREACH OF WARRANTY. THE MANUFACTURER OR INSTALLER WILL, AT ITS ELECTION, EITHER (i) REPAIR OR REPLACE THE SOFTWARE AT NO CHARGE, OR (ii) ACCEPT RETURN OF THE PRODUCT(S) FOR A REFUND OF THE AMOUNT PAID, IF ANY. THE MANUFACTURER OR INSTALLER MAY ALSO REPAIR OR REPLACE SUPPLEMENTS, UPDATES AND REPLACEMENT SOFTWARE OR PROVIDE A REFUND OF THE AMOUNT YOU PAID FOR THEM, IF ANY. CONTACT THE MANUFACTURER OR INSTALLER ABOUT ITS POLICY. THESE ARE YOUR ONLY REMEDIES FOR BREACH OF THE LIMITED WARRANTY.

E. CONSUMER RIGHTS NOT AFFECTED. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS, WHICH THIS AGREEMENT CANNOT CHANGE.

F. WARRANTY PROCEDURES. Contact the manufacturer or installer to find out how to obtain warranty service for the software. For a refund, you must comply with the manufacturer's or installer's return policies.

G. NO OTHER WARRANTIES. THE LIMITED WARRANTY IS THE ONLY DIRECT WARRANTY FROM THE MANUFACTURER OR INSTALLER, OR MICROSOFT. THE MANUFACTURER, OR INSTALLER AND MICROSOFT GIVE NO OTHER EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. WHERE ALLOWED BY YOUR LOCAL LAWS, THE MANUFACTURER OR INSTALLER AND MICROSOFT EXCLUDE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. If your local laws give you any implied warranties, guarantees or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

H. LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. THE LIMITATION ON AND EXCLUSION OF DAMAGES CLAUSE ABOVE APPLIES TO BREACHES OF THIS LIMITED WARRANTY. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE. YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM COUNTRY TO COUNTRY.

3. PRODUCT KEY CARD TERMS

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software which (i) was initially preinstalled on your device and (ii) which is named on the PRODUCT KEY CARD you have purchased in order to convert the trial rights into perpetual rights. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

IF YOU DO NOT ACCEPT THE LICENSE TERMS, DO NOT USE THE SOFTWARE. INSTEAD, RETURN YOUR PRODUCT KEY CARD TO YOUR PLACE OF PURCHASE FOR A REFUND OR CREDIT. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft's refund policies. See www.microsoft.com/worldwide. In the United States and Canada, call (800) MICROSOFT or see www.microsoft.com/info/nareturns.htm.

AS DESCRIBED BELOW, USING THE SOFTWARE ALSO OPERATES AS YOUR CONSENT TO THE TRANSMISSION OF CERTAIN COMPUTER INFORMATION DURING ACTIVATION, VALIDATION AND FOR INTERNET-BASED SERVICES.

IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW FOR EACH LICENSE YOU ACQUIRE.

1. OVERVIEW. The software is licensed on a per copy per device basis. A hardware partition or blade is considered to be a separate device.

2. INSTALLATION AND USE RIGHTS.

a. One Copy per Device. The software license is permanently assigned to the device on which the software is initially activated. That device is the "licensed device."

b. Licensed Device. You may only use one copy of the software on the licensed device at a time.

c. Separation of Components. The components of the software are licensed as a single unit. You may not separate the components and install them on different devices.

d. Alternative Versions. The software may include more than one version, such as 32-bit and 64-bit. You may use only one version at one time.

3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Multiplexing. Hardware or software you use to

- pool connections,
 - reroute information, or
 - reduce the number of devices or users that directly access or use the software
- (sometimes referred to as "multiplexing" or "pooling"), does not reduce the number of licenses you need.

b. Font Components. While the software is running, you may use its fonts to display and print content. You may only

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to help print content.

c. Media Elements and Templates. You may have access to media images, clip art, animations, sounds, music, video clips, templates and other forms of content ("media elements") provided with the software or as part of a service associated with the software. You may copy and use the media

elements in projects and documents. You may not (i) sell, license or distribute copies of the media elements by themselves or as a product if the primary value of the product is the media elements; (ii) grant your customers rights to further license or distribute the media elements; (iii) license or distribute for commercial purposes media elements that include the representation of identifiable individuals, governments, logos, trademarks, or emblems or use these types of images in ways that could imply an endorsement or association with your product, entity or activity; or (iv) create obscene or scandalous works using the media elements. For more information, go to www.microsoft.com/permission.

d. Use with Virtualization Technologies. Instead of using the software directly on the licensed device, you may install and use the software within only one virtual (or otherwise emulated) hardware system on the licensed device.

e. Remote Access. The single primary user of the licensed device may access and use the software installed on the licensed device remotely from any other device. You may allow others to access the software to provide you with support services. You do not need additional licenses for this access. No other person may use the software under the same license at the same time for any other purpose.

f. Development Tools. The software may contain Microsoft Visual Studio Tools for Applications or other development tools. You may use any development tools included in the software only to design, develop, test, use and demonstrate your programs with the software.

g. Language Version Selection. If you are provided with a one-time selection between language versions, without a language pack or LIP, you may use only the one language version you select. If you were not provided with a language selection, the language version will default to the language of your operating system or, if your operating system language is not available, to another available language. If you are provided with a language pack or LIP, your use of language versions is not limited. A "LIP" is a Language Interface Pack. Language packs and LIPs offer additional language version support of the software. The language packs and LIPs are a part of the software, and may not be used separately.

h. Trial and Conversion. Some or all of the software may be licensed on a trial basis. Your rights to use trial software are limited to the trial period. The trial software and length of the trial period are set forth during the activation process. You may have the option to convert your trial rights to subscription or perpetual rights. Conversion options will be presented to you at the expiration of your trial period. After the expiration of any trial period without conversion, most features of the trial software will stop running. At that time you can continue to open, view and print any documents you created with the trial software.

i. Subscription Software. If you licensed the software on a subscription basis, your rights to use the software are limited to the subscription period. You may have the option to extend your subscription or convert to a perpetual license. If you extend your subscription, you may continue using the software until the end of your extended subscription period. See

the software activation screens or other accompanying materials for subscription details. After the expiration of your subscription, most features of the software will stop running. At that time you can continue to open, view and print any documents you created with the software.

4. MANDATORY ACTIVATION. Activation associates the use of the software with a specific device. During activation, the software will send information about the software and the device to Microsoft. This information includes the version, the license version, language and product key of the software, the Internet protocol address of the device, and information derived from the hardware configuration of the device. For more information, see www.microsoft.com/piracy/activation.msp. BY USING THE SOFTWARE, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. If properly licensed, you have the right to use the version of the software installed during the installation process up to the time permitted for activation. UNLESS THE SOFTWARE IS ACTIVATED, YOU HAVE NO RIGHT TO USE THE SOFTWARE AFTER THE TIME PERMITTED FOR ACTIVATION. This is to prevent its unlicensed use. YOU ARE NOT PERMITTED TO BYPASS OR CIRCUMVENT ACTIVATION. You can activate the software by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. THE SOFTWARE WILL REMIND YOU TO ACTIVATE IT UNTIL YOU DO.

5. VALIDATION.

a. The software will from time to time request download of the validation feature of the software. Validation verifies that the software has been activated and is properly licensed. A validation check confirming that you are properly licensed permits you to use the software, certain features of the software or to obtain additional benefits. For more information, see www.microsoft.com/genuine/office/WhyValidate.aspx.

b. During or after a validation check, the software may send information about the software, the device and the results of the validation check to Microsoft. This information includes, for example, the version and product key of the software and the Internet protocol address of the licensed device. Microsoft does not use the information to identify or contact you. BY USING THE SOFTWARE, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. For more information about validation and what is sent during or after a validation check, see www.microsoft.com/genuine/office/PrivacyInfo.aspx.

c. If, after a validation check, the software is found to be counterfeit, improperly licensed, or a non-genuine Office product then the functionality or experience of using the software may be affected. For example, Microsoft may

- provide notice that the software is improperly licensed or a non-genuine Office product; and you may
 - receive reminders to obtain a properly licensed copy of the software; or
 - need to follow Microsoft's instructions to be licensed to use the software and reactivate;
- and you may not be able to
- use or continue to use the software or some of the features of the software; or

- obtain certain updates or upgrades from Microsoft.

d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources, see www.microsoft.com/genuine/downloads/faq.aspx.

6. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

a. Consent for Internet-Based Services. The software features described below and in the Office 2010 Privacy Statement connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. In some cases, you may switch off these features or not use them. For more information about these features, see the Office 2010 Privacy Statement at r.office.microsoft.com/r/rlidOOClientPrivacyStatement14?clid=1033. BY USING THESE FEATURES, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. Microsoft does not use the information to identify or contact you.

Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the device where you installed the software. Microsoft uses this information to make the Internet-based services available to you.

- Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance and help. You may choose not to use these web content features.

- Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists using the Internet, when available.

- SharePoint Workspace. If the software includes Microsoft SharePoint Workspace ("SharePoint Workspace"), SharePoint Workspace will allow you to communicate directly with others over the Internet. If you cannot communicate directly with a contact over the Internet, and your administrator uses Microsoft's public server infrastructure, your communications will be encrypted and sent through Microsoft servers for later delivery. You cannot disable this service if your administrator uses Microsoft's public server infrastructure.

SharePoint Workspace makes some information about your SharePoint Workspace account and device known to your approved contacts. For example, if you:

- add a contact to your contact list,
- import your user account onto a new device,
- update the information in your "identity contact", or
- send a SharePoint Workspace invitation using an URL to reference the invitation file, information about you and your devices may be sent to your contacts. If you configure SharePoint Workspace to use Microsoft servers, those servers will collect information about your device and user accounts.

b. Automatic Update. Software with Click-to-Run technology may periodically check with Microsoft for updates and supplements to the software. If found, these updates and supplements might be automatically downloaded and installed on your licensed device.

c. Use of Information. Microsoft may use the device information, error reports, and malware reports to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

d. Misuse of Internet-based Services. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

7. SCOPE OF LICENSE. The software is licensed, not sold. This agreement only gives you some rights to use the features included in the software edition you licensed. Microsoft reserve reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- use the software in any way that is against the law;
- use components of the software to run applications not running on the software;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

8. BACKUP COPY. You may order or download a backup copy of the software from www.microsoft.com/office/backup/. You may not distribute the backup copy of the software. You may use it only to reinstall the software on the license device.

9. DOCUMENTATION. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

10. NOT FOR RESALE SOFTWARE. You may not sell software marked as "NFR" or "Not for Resale."

11. HOME AND STUDENT SOFTWARE. For software marked "Home and Student" edition, you may not use the software for any commercial, non-profit, or revenue-generating activities.

12. GEOGRAPHIC RESTRICTIONS. If the software is marked as requiring activation in a specific geographic region, then you are only permitted to activate this software in the geographic region indicated on the

software or computer packaging. You may not be able to activate the software outside of that region. For further information on geographic restrictions, visit go.microsoft.com/fwlink/?LinkId=141397.

13. UPGRADE OR CONVERSION. To upgrade or convert software, you must first be licensed for the software that is eligible for the upgrade or conversion. Upon upgrade or conversion, this agreement takes the place of the agreement for the software you upgraded or converted from. After you upgrade or convert, you may no longer use the software you upgraded or converted from.

14. PROOF OF LICENSE.

a. If you acquired the Product Key Card, your proof of license is the genuine Microsoft certificate of authenticity label with the accompanying genuine product key card and your proof of purchase from an authorized electronic supplier of genuine Microsoft software. To be valid, this label must be attached to the product key card. If you receive the label separately, it is invalid. Proof of purchase may be subject to verification by your merchant's records.

b. To identify genuine Microsoft software, see www.howtotell.com.

15. TRANSFER TO A THIRD PARTY. You may transfer the software directly to a third party only with the licensed device, the Certificate of Authenticity label, and this agreement. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. You may not retain any copies.

16. EXPORT RESTRICTIONS. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

17. SUPPORT SERVICES. Microsoft provides support services for the software as described at www.support.microsoft.com/common/international.aspx. If you are using software that is not properly licensed, you will not be entitled to receive support services.

18. ENTIRE AGREEMENT. This agreement (including the warranty below), additional terms (including any printed-paper license terms that accompany the software, and may modify or replace some or all of these terms), and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

19. APPLICABLE LAW.

a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the software in any other country, the laws of that country apply.

20. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

21. LIMITATION ON AND EXCLUSION OF DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO THE AMOUNT YOU PAID FOR THE SOFTWARE. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES. This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if

- repair, replacement or a refund for the software does not fully compensate you for any losses; or
- the manufacturer or installer, or Microsoft knew or should have known about the possibility of the damages.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

LIMITED WARRANTY

A. LIMITED WARRANTY. If you follow the instructions, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

B. TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. THE LIMITED WARRANTY COVERS THE SOFTWARE FOR ONE YEAR AFTER ACQUIRED BY THE FIRST USER. IF YOU RECEIVE SUPPLEMENTS, UPDATES, OR REPLACEMENT SOFTWARE DURING THAT YEAR, THEY WILL BE COVERED FOR THE REMAINDER OF THE WARRANTY OR 30 DAYS, WHICHEVER IS LONGER. If the first user transfers the software, the remainder of the warranty will apply to the recipient. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES, GUARANTEES OR CONDITIONS LAST ONLY DURING THE TERM OF THE LIMITED WARRANTY. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee or condition lasts.

C. EXCLUSIONS FROM WARRANTY. This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond Microsoft's reasonable control.

D. REMEDY FOR BREACH OF WARRANTY. MICROSOFT WILL REPAIR OR REPLACE THE

SOFTWARE AT NO CHARGE. IF MICROSOFT CANNOT REPAIR OR REPLACE IT, MICROSOFT WILL REFUND THE AMOUNT SHOWN ON YOUR RECEIPT FOR THE SOFTWARE. IT WILL ALSO REPAIR OR REPLACE SUPPLEMENTS, UPDATES AND REPLACEMENT SOFTWARE AT NO CHARGE. IF MICROSOFT CANNOT REPAIR OR REPLACE THEM, IT WILL REFUND THE AMOUNT YOU PAID FOR THEM, IF ANY. YOU MUST UNINSTALL THE SOFTWARE AND RETURN ANY MEDIA AND OTHER ASSOCIATED MATERIALS TO MICROSOFT WITH PROOF OF PURCHASE TO OBTAIN A REFUND. THESE ARE YOUR ONLY REMEDIES FOR BREACH OF THE LIMITED WARRANTY.

E. CONSUMER RIGHTS NOT AFFECTED. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS, WHICH THIS AGREEMENT CANNOT CHANGE.

F. WARRANTY PROCEDURES. You need proof of purchase for warranty service.

1. United States and Canada. For warranty service or information about how to obtain a refund for software acquired in the United States and Canada, contact Microsoft at

- (800) MICROSOFT;
- Microsoft Customer Service and Support, One Microsoft Way, Redmond, WA 98052-6399; or
- Visit www.microsoft.com/info/nareturns.htm.

2. Europe, Middle East and Africa. If you acquired the software in Europe, the Middle East or Africa, Microsoft Ireland Operations Limited makes this limited warranty. To make a claim under this warranty, you should contact either

- Microsoft Ireland Operations Limited, Customer Care Centre, Atrium Building Block B, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Ireland; or
- the Microsoft affiliate serving your country (see www.microsoft.com/worldwide).

3. Outside United States, Canada, Europe, Middle East and Africa. If you acquired the software outside the United States, Canada, Europe, the Middle East and Africa, contact the Microsoft affiliate serving your country (see www.microsoft.com/worldwide).

G. NO OTHER WARRANTIES. THE LIMITED WARRANTY IS THE ONLY DIRECT WARRANTY FROM MICROSOFT. MICROSOFT GIVES NO OTHER EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. WHERE ALLOWED BY YOUR LOCAL LAWS, MICROSOFT EXCLUDES IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. If your local laws give you any implied warranties, guarantees or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

H. LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. THE LIMITATION ON AND EXCLUSION OF DAMAGES CLAUSE ABOVE APPLIES TO BREACHES OF THIS LIMITED WARRANTY.

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE. YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM COUNTRY TO COUNTRY.

EULAIID:014_RTM_CLT.1_RTM_EN

VMWARE END USER LICENSE AGREEMENT

VMware End User License Agreement

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party, an entity that is directly or indirectly controlled by or is under common control with such party, where "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the relevant entity (but only as long as such person or entity meets these requirements).

1.2 "Documentation" means that documentation that is generally provided to You by VMware with the Software, as revised by VMware from time to time, and which may include end user manuals, operation instructions, installation guides, release notes, and on-line help files regarding the use of the Software.

1.3 "Guest Operating Systems" means instances of third-party operating systems licensed by You, installed in a Virtual Machine and run using the Software.

1.4 "Intellectual Property Rights" means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know how, inventions, patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.

1.5 "License" means a license granted under Section 2.1.

1.6 "License Key" means a serial number that enables You to activate and use the Software.

1.7 “License Term” means the duration of a License as specified in the Order.

1.8 “License Type” means the type of License applicable to the Software, as more fully described in the Order.

1.9 “Open Source Software” or “OSS” means software components that are licensed under a license approved by the Open Source Initiative (“OSI”) or similar open source or freeware license and are embedded in the delivered Software.

1.10 “Order” means a purchase order, enterprise license agreement, or other ordering document issued by You to VMware or a VMware authorized reseller that references and incorporates this EULA and is accepted by VMware as set forth in Section 4.

1.11 “Product Guide” means the current version of the VMware Product Guide at the time of Your Order, copies of which are found at www.vmware.com/download/eula.

1.12 “Services Terms” means VMware’s then-current Support and Subscription Contract Terms and Conditions, copies of which are found at www.vmware.com/files/pdf/support/support_terms_conditions.pdf.

1.13 “Software” means the VMware Tools and the VMware computer programs listed on VMware’s commercial price list to which You acquire a license under an Order, together with any software code relating to the foregoing that is provided to You pursuant to a support and subscription service contract and that is not subject to a separate license agreement.

1.14 “Territory” means the country or countries in which You have been invoiced; provided, however, that if You have been invoiced within any of the European Economic Area member states, You may deploy the corresponding Software throughout the European Economic Area.

1.15 “Third Party Agent” means a third party delivering information technology services to You pursuant to a written contract with You.

1.16 “Virtual Machine” means a software container that can run its own operating system and execute applications like a physical machine.

1.17 “VMware” means VMware, Inc., a Delaware corporation, if You are purchasing Licenses or services for use in the United States and VMware International Limited, a company organized and existing under the laws of Ireland, for all other purchases.

1.18 “VMware Tools” means the suite of utilities and drivers, Licensed by VMware under the “VMware Tools” name, that can be installed in a Guest Operating System to enhance the performance and functionality of a Guest Operating System when running in a Virtual Machine.

2. LICENSE GRANT.

2.1 Scope of License. Subject to the terms and conditions of this EULA, VMware grants You, during the License Term, a non-exclusive, non-transferable License to use the Software, in

executable code form only, within the Territory, for Your internal operations in accordance with (a) the Documentation; (b) the License Type for which You have paid the applicable fees; (c) other applicable limitations set forth in the Order. The License to the Software is limited to the quantities specified in each applicable Order.

2.2 Third Party Use. Under the License granted to You in Section 2.1 above, You may permit Your Third Party Agents to access, use and/or operate the Software on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents' compliance with terms and conditions of this EULA and any breach of this EULA by a Third Party Agent shall be deemed to be a breach by You.

2.3 Permitted Copies. You may make one copy of the Software for archival purposes only. The copy shall: (a) be kept within Your possession or control; (b) include all titles, trademarks, and copyright and restricted rights notices in the original; and (c) be subject to this EULA. You may not otherwise copy the Software without VMware's prior written consent.

2.4 Benchmarking. You may use the Software to conduct internal performance testing and benchmarking studies. You may only publish or otherwise distribute the results of such studies to third parties as follows: (a) if with respect to VMware's Workstation or Fusion products, only if You provide a copy of Your study to benchmark@vmware.com prior to distribution; (b) if with respect to any other Software, only if VMware has reviewed and approved of the methodology, assumptions and other parameters of the study (please contact VMware at benchmark@vmware.com to request such review and approval) prior to such publication and distribution.

2.5 VMware Tools. You may distribute the VMware Tools (whether or not as part of the Virtual Machine You create with the Software) to third parties solely when installed in a Guest Operating System to enhance its performance and functionality when running in a Virtual Machine, provided that You will be fully responsible for such third parties' compliance with the terms and conditions of this EULA, and any breach of this EULA by any such third party shall be deemed to be a breach of this EULA by You.

2.6 Open Source Software. Notwithstanding anything herein to the contrary, Open Source Software is licensed to You under such OSS's own applicable license terms, which can be found in the `open_source_licenses.txt` file, the Documentation or as applicable, the corresponding source files for the Software available at www.vmware.com/download/open_source.html. These OSS license terms are consistent with the license granted in Section 2, and may contain additional rights benefiting You. The OSS license terms shall take precedence over this EULA to the extent that this EULA imposes greater restrictions on You than the applicable OSS license terms.

3. RESTRICTIONS; OWNERSHIP.

3.1 Restrictions. You acknowledge that the Software and the structure, organization and source code of the Software constitute valuable trade secrets of VMware. Accordingly, except as expressly permitted in Section 2 or as otherwise authorized by VMware in writing, You will not and will not permit any third party to: (a) sell, lease, license, distribute, sublicense or otherwise

transfer in whole or in part the Software or Documentation to any third party; (b) decompile, disassemble, reverse engineer, or otherwise attempt to derive source code from the Software, in whole or in part; (c) copy the Software, except for archival purposes, as set out in Section 2.3; (d) create, develop, license, install, use, or deploy any software or services to circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Software as described in this EULA; (e) translate, modify or create derivative works based upon the Software; (f) permit any use of or access to the Software by any third party; (g) remove any product identification, proprietary, copyright or other notices contained in the Software; or (h) operate the Software on behalf of or for the benefit of any third party, including the operation of any service that is accessed by a third party, except that, for the purposes of this Section 3.1 (h), You may use the Software to deliver hosted services to Your Affiliates.

3.2 Decompilation. Notwithstanding the foregoing, decompiling the Software is permitted to the extent the laws of the Territory give You the express right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, You must first request such information from VMware (at info@vmware.com), provide all reasonably requested information to allow VMware to assess Your claim, and VMware may, in its discretion, either provide such interoperability information to You, impose reasonable conditions, including a reasonable fee, on such use of the Software, or offer to provide alternatives to ensure that VMware's proprietary rights in the Software are protected and to reduce any adverse impact on VMware's proprietary rights.

3.3 Ownership. The Software and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Software and Documentation shall be limited to those expressly granted in this EULA and any applicable Order. No other rights with respect to the Software or any related Intellectual Property Rights are implied. You are not authorized to use (and shall not permit any third party to use) the Software, Documentation or any portion thereof except as expressly authorized by this EULA or the applicable Order.

3.4 Guest Operating Systems. Certain Software allows Guest Operating Systems and application programs to run on a computer system. You acknowledge that You are responsible for obtaining and complying with any licenses necessary to operate any such third-party software.

4. ORDER. Your Order is subject to this EULA. No Orders are binding on VMware until accepted by VMware. Orders for Software are deemed to be accepted upon VMware's delivery of the Software included in such Order. Orders issued to VMware do not have to be signed to be valid and enforceable.

5. AUDIT RIGHTS.

5.1 Records. You will, during the License Term for any Software licenses acquired under this EULA (and for a period of two (2) years from the expiration of the applicable License Term), maintain accurate records of your use of the Software sufficient to demonstrate Your compliance with the terms of this EULA and all Orders.

5.2 Audit Rights. During the period in which the You are obligated to maintain such records, VMware, or its third party auditor, may, upon reasonable notice to You, audit such records to verify that You have (a) used the Software solely in the manner authorized herein; (b) paid all applicable license fees; and (c) otherwise complied with the terms of this EULA and all Orders. VMware may conduct no more than one (1) audit in any twelve (12) month period. Audits will be conducted during normal business hours and VMware will use commercially reasonable efforts to minimize the disruption of Your normal business activities. VMware, and any third-party auditor, shall not have physical access to Your computing devices in connection with any such audit, without Your prior written consent. You will reasonably cooperate with VMware and/or its third-party auditor and will promptly pay directly to VMware any underpayments revealed by such audit. You will promptly reimburse VMware for all reasonable costs and expenses incurred by VMware for such audit if: (i) such audit reveals an underpayment by You of more than five percent (5%) of the fees payable by You to VMware for the period audited, or (ii) such audit reveals You have materially failed to maintain accurate records of Your use of the Software.

6. SUPPORT AND SUBSCRIPTION SERVICES. Except as expressly specified in the Product Guide, VMware does not provide any support or subscription services for the Software under this EULA. You have no rights to any updates, upgrades or extensions or enhancements to the Software developed by VMware unless you separately purchase VMware support or subscription services. These support or subscription services are subject to the Services Terms.

7. WARRANTIES.

7.1 Software Warranty. VMware warrants to You that the Software will, for a period of ninety (90) days following delivery ("**Warranty Period**"), substantially conform to the applicable Documentation, provided that the Software (a) has been properly installed and used at all times and in accordance with the applicable Documentation; and (b) has not been modified or added to by persons other than VMware or its authorized representative. VMware will, at its own expense and as its sole obligation and Your exclusive remedy for any breach of the foregoing warranty, either replace the applicable Software or correct any reproducible error in the Software reported to VMware by You in writing during the Warranty Period. If VMware determines that it is unable to correct the error or replace the Software, VMware will refund to You all License fees actually paid by You, in which case the License for the applicable Software and Your right to use such Software will terminate.

7.2 Disclaimer of Warranties. THE EXPRESS WARRANTY IN SECTION 7.1 ABOVE IS IN LIEU OF AND, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS LICENSORS DISCLAIM, ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE) REGARDING OR RELATING TO THE SOFTWARE, THE DOCUMENTATION, OR ANY MATERIALS FURNISHED OR PROVIDED TO YOU UNDER THIS EULA. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM

DEFECTS OR THAT THE SOFTWARE WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

8. INTELLECTUAL PROPERTY INDEMNIFICATION.

8.1 Defense and Indemnification. Subject to the remainder of this Section 8, VMware shall defend You against any third party claim that the Software infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that such misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) the People's Republic of China, to the extent that such countries are part of the Territory for the License (**"Infringement Claim"**) and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement; provided that You: (i) promptly provide VMware with notice of such Infringement Claim; (ii) allow VMware sole control over the defense thereof and related settlement negotiation; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware.

8.2 Remedies. Should the Software become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense either: (a) procure the rights necessary for You to make continued use of the affected Software in accordance with this EULA; (b) replace or modify the affected Software to make it non-infringing; or (c) terminate the License to the affected Software and discontinue the related support services, and, upon Your certified deletion of the affected Software, refund: (i) the fees paid by You for the License to the affected Software, less straight-line depreciation over a three (3) year useful life beginning on the date such Software was delivered; and (ii) any pre-paid service fee attributable to related support services to be delivered after the date such service is stopped. Nothing in this Section 8.2 shall limit VMware's obligation under Section 8.1 to defend and indemnify You, provided that You replace the allegedly infringing Software upon VMware's making alternate Software available to You and/or You discontinue using the allegedly infringing Software upon receiving VMware's notice terminating the affected License.

8.3 Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 8 or otherwise with respect to any claim based on: (a) a combination of Software with non-VMware products (other than non-VMware products that are listed on the Order and used in an unmodified form); (b) use for a purpose or in a manner for which the Software was not designed; (c) use of any older version of the Software when use of a newer VMware revision would have avoided the infringement; (d) any modification to the Software made without VMware's express written approval; (e) any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by VMware into Software listed on VMware's commercial price list; (f) any claim that relates to Linux or Android open source software, even when it has been embedded into or distributed with the Software or (g) any Software provided on a no charge, beta or evaluation basis. **THIS SECTION 8 STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.**

9. LIMITATION OF LIABILITY.

9.1 Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS EULA WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE LICENSE FEES YOU PAID FOR THE SOFTWARE, IF ANY. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

9.2 Further Limitations. VMware's licensors shall have no liability of any kind under this EULA and VMware's liability with respect to any third party software embedded in the Software shall be subject to Section 9.1. You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises.

10. TERMINATION.

10.1 License Term. This EULA will terminate in its entirety upon the termination of the License Term, unless terminated earlier under this Section 10.

10.2 Termination for Breach. VMware may terminate this EULA in its entirety effective immediately upon written notice to You if: (a) You breach any provision in Section 3 and do not cure the breach within ten (10) days after receiving written notice thereof from VMware; (b) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; (c) You breach any other provision of this EULA and don't not cure the breach within thirty (30) days after receiving written notice thereof from VMware; or (d) You commit a material breach that is not capable of being cured.

10.3 Termination for Insolvency. VMware may terminate this EULA in its entirety effective immediately upon written notice to You if You: (a) terminate or suspend your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding.

10.4 Effect of Termination. If VMware terminates this EULA under this Section 10: (a) all Licensed rights to all Software granted to You under this EULA will immediately cease to exist; and (b) You must promptly discontinue all use of all Software, and (destroy all copies of the

Software and all License Key(s)) and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Sections 1 (Definitions), 2.6 (Open Source Software), 3 (Restrictions; Ownership), 5.1 (Records), 5.2 (Audit Rights), 7.2 (Disclaimer of Warranties), 9 (Limitation of Liability), 10 (Termination), 11 (Confidential Information) and 12 (General) will any survive termination of this EULA.

11. CONFIDENTIAL INFORMATION.

11.1 Definition. “Confidential Information” means information or materials provided by one party (“Discloser”) to the other party (“Recipient”) which are in tangible form and labeled “confidential” or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) License Keys; (b) information regarding VMware’s pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Software.

11.2 Protection. Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this EULA; or (b) in connection with the parties’ ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by the EULA, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for purposes of the EULA and who are under a duty of confidentiality no less restrictive than Recipient’s duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

11.3 Exceptions. Recipient’s obligations under Section 11.2 with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser’s Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser’s request and expense, in any lawful action to contest or limit the scope of such required disclosure.

11.4 Data Privacy. You agree that VMware may process technical and related information about Your use of the Software which may include internet protocol address, hardware identification, operating system, application software, peripheral hardware, and non-personally identifiable Software usage statistics to facilitate the provisioning of updates, support, invoicing or online services and may transfer such information to other companies in the VMware worldwide group of companies from time to time. To the extent that this information constitutes personal data, VMware shall be the controller of such personal data. To the extent that it acts as a controller,

each party shall comply at all times with its obligations under the local legislation applicable in the Territory for the protection of individuals with regard to the processing of personal data. Collected data is subject to VMware's Privacy Policy at <http://www.vmware.com/help/privacy.html>.

12. GENERAL.

12.1 Assignment. This EULA and any Orders, and any of Your rights or obligations thereunder, may not be assigned, subcontracted or transferred by You, in whole or in part, whether voluntary, by operation of contract, law or otherwise, without the prior written consent of VMware. Any attempted assignment or transfer in violation of the foregoing will be null and void. Subject to the foregoing, this EULA will be binding upon and will inure to the benefit of the parties and their respective successors and assigns.

12.2 Notices. Any notice delivered by VMware to You under this EULA will be delivered via mail, email or fax.

12.3 Waiver. The waiver of a breach of any provision of this EULA shall not constitute a waiver of any other provision or any subsequent breach.

12.4 Severability. If any provision of this EULA is held to be illegal, invalid or unenforceable, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this EULA will remain in full force and effect.

12.5 Compliance with Laws; Export Control; Government Regulations. Each party shall comply with all laws applicable to the actions contemplated by this EULA. You acknowledge that the Software is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) you are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) you will not permit the Software to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and documentation by the U.S. Government shall be governed solely by the terms and conditions of this EULA.

12.6 Construction. The headings of sections of this EULA are for convenience and are not to be used in interpreting this EULA. As used in this EULA, the word 'including' means "including but not limited to."

12.7 Governing Law. This EULA is governed by the laws of the State of California, United States of America, unless mandated by other law. The United Nations Convention for the International Sale of Goods shall not apply.

12.8 Third Party Rights. Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.

12.9 Product Guide. In addition to the above sections, Your use of the Software is subject to the terms and conditions of the Product Guide, which is incorporated herein by reference.

12.10 Order of Precedence. In the event of conflict or inconsistency among the Product Guide, this EULA and the Order, the following order of precedence shall apply: (a) the Product Guide, (b) this EULA and (c) the Order. With respect to any inconsistency between this EULA and an Order, the terms of this EULA shall supersede and control over any conflicting or additional terms and conditions of any Order, acknowledgement or confirmation or other document issued by You, unless the parties execute a written agreement expressly indicating: (i) that such Order shall modify this EULA; or (ii) that the terms of such Order shall supersede and control in the event of any inconsistency.

12.11 Entire Agreement. This EULA, including accepted Orders and any amendments hereto, and the Product Guide contain the entire agreement of the parties with respect to the subject matter of this EULA and supersede all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This EULA may be amended only in writing signed by authorized representatives of both parties.

12.12 Contact Information. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America. If You have any questions concerning this EULA, please send an email to info@vmware.com.

- See more at:

http://www.vmware.com/download/eula/universal_eula.html#sthash.NSO0dWUO.dpuf

VMWARE vSPHERE END USER LICENSE AGREEMENT

VMware vSphere End User License Agreement

Effective August 27, 2012, VMware is eliminating the vRAM restriction on licenses to VMware vSphere. The removal of the vRAM limit from VMware vSphere licenses applies retroactively to any past and existing users of VMware vSphere, in addition to any new users of VMware vSphere. This new policy replaces and supersedes any conflicting terms in any license agreement previously agreed upon between VMware and any licensee of VMware vSphere. This change does not apply to VMware vSphere users under the VMware Service Provider Program.

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY:BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party, an entity that is directly or indirectly controlled by or is under common control with such party, where "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the relevant entity (but only as long as such person or entity meets these requirements).

1.2 "Documentation" means that documentation that is generally provided to You by VMware with the Software, as revised by VMware from time to time, and which may include end user manuals, operation instructions, installation guides, release notes, and on-line help files regarding the use of the Software.

1.3 "Guest Operating Systems" means instances of third-party operating systems licensed by You, installed in a Virtual Machine and run using the Software.

1.4 "Intellectual Property Rights" means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know how, inventions,

patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.

1.5 “License” means a license granted under Section 2.1.

1.6 “License Key” means a serial number that enables You to activate and use the Software.

1.7 “License Term” means the duration of a License as specified in the Order.

1.8 “License Type” means the type of License applicable to the Software, as more fully described in the Order.

1.9 “Open Source Software” or “OSS” means software components that are licensed under a license approved by the Open Source Initiative (“OSI”) or similar open source or freeware license and are embedded in the delivered Software.

1.10 “Order” means a purchase order, enterprise license agreement, or other ordering document issued by You to VMware or a VMware authorized reseller that references and incorporates this EULA and is accepted by VMware as set forth in Section 4.

1.11 “Product Guide” means the current version of the VMware Product Guide at the time of Your Order, copies of which are found at www.vmware.com/download/eula.

1.12 “Services Terms” means VMware’s then-current Support and Subscription Contract Terms and Conditions, copies of which are found at www.vmware.com/files/pdf/support/support_terms_conditions.pdf.

1.13 “Software” means the VMware Tools and the VMware computer programs listed on VMware’s commercial price list to which You acquire a license under an Order, together with any software code relating to the foregoing that is provided to You pursuant to a support and subscription service contract and that is not subject to a separate license agreement.

1.14 “Territory” means the country or countries in which You have been invoiced; provided, however, that if You have been invoiced within any of the European Economic Area member states, You may deploy the corresponding Software throughout the European Economic Area.

1.15 “Third Party Agent” means a third party delivering information technology services to You pursuant to a written contract with You.

1.16 “Virtual Machine” means a software container that can run its own operating system and execute applications like a physical machine.

1.17 “VMware” means VMware, Inc., a Delaware corporation, if You are purchasing Licenses or services for use in the United States and VMware International Limited, a company organized and existing under the laws of Ireland, for all other purchases.

1.18 “VMware Tools” means the suite of utilities and drivers, Licensed by VMware under the “VMware Tools” name, that can be installed in a Guest Operating System to enhance the performance and functionality of a Guest Operating System when running in a Virtual Machine.

2. LICENSE GRANT.

2.1 Scope of License. Subject to the terms and conditions of this EULA, VMware grants You, during the License Term, a non-exclusive, non-transferable License to use the Software, in executable code form only, within the Territory, for Your internal operations in accordance with (a) the Documentation; (b) the License Type for which You have paid the applicable fees; (c) other applicable limitations set forth in the Order. The License to the Software is limited to the quantities specified in each applicable Order.

2.2 Third Party Use. Under the License granted to You in Section 2.1 above, You may permit Your Third Party Agents to access, use and/or operate the Software on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents’ compliance with terms and conditions of this EULA and any breach of this EULA by a Third Party Agent shall be deemed to be a breach by You.

2.3 Permitted Copies. You may make one copy of the Software for archival purposes only. The copy shall: (a) be kept within Your possession or control; (b) include all titles, trademarks, and copyright and restricted rights notices in the original; and (c) be subject to this EULA. You may not otherwise copy the Software without VMware’s prior written consent.

2.4 Benchmarking. You may use the Software to conduct internal performance testing and benchmarking studies. You may only publish or otherwise distribute the results of such studies to third parties as follows: (a) if with respect to VMware’s Workstation or Fusion products, only if You provide a copy of Your study to benchmark@vmware.com prior to distribution; (b) if with respect to any other Software, only if VMware has reviewed and approved of the methodology, assumptions and other parameters of the study (please contact VMware at benchmark@vmware.com to request such review and approval) prior to such publication and distribution.

2.5 VMware Tools. You may distribute the VMware Tools (whether or not as part of the Virtual Machine You create with the Software) to third parties solely when installed in a Guest Operating System to enhance its performance and functionality when running in a Virtual Machine, provided that You will be fully responsible for such third parties’ compliance with the terms and conditions of this EULA, and any breach of this EULA by any such third party shall be deemed to be a breach of this EULA by You.

2.6 Open Source Software. Notwithstanding anything herein to the contrary, Open Source Software is licensed to You under such OSS’s own applicable license terms, which can be found in the open_source_licenses.txt file, the Documentation or as applicable, the corresponding source files for the Software available at www.vmware.com/download/open_source.html. These

OSS license terms are consistent with the license granted in Section 2, and may contain additional rights benefiting You. The OSS license terms shall take precedence over this EULA to the extent that this EULA imposes greater restrictions on You than the applicable OSS license terms.

3. RESTRICTIONS; OWNERSHIP.

3.1 Restrictions. You acknowledge that the Software and the structure, organization and source code of the Software constitute valuable trade secrets of VMware. Accordingly, except as expressly permitted in Section 2 or as otherwise authorized by VMware in writing, You will not and will not permit any third party to: (a) sell, lease, license, distribute, sublicense or otherwise transfer in whole or in part the Software or Documentation to any third party; (b) decompile, disassemble, reverse engineer, or otherwise attempt to derive source code from the Software, in whole or in part; (c) copy the Software, except for archival purposes, as set out in Section 2.3; (d) create, develop, license, install, use, or deploy any software or services to circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Software as described in this EULA; (e) translate, modify or create derivative works based upon the Software; (f) permit any use of or access to the Software by any third party; (g) remove any product identification, proprietary, copyright or other notices contained in the Software; or (h) operate the Software on behalf of or for the benefit of any third party, including the operation of any service that is accessed by a third party, except that, for the purposes of this Section 3.1 (h), You may use the Software to deliver hosted services to Your Affiliates.

3.2 Decompilation. Notwithstanding the foregoing, decompiling the Software is permitted to the extent the laws of the Territory give You the express right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, You must first request such information from VMware (at info@vmware.com), provide all reasonably requested information to allow VMware to assess Your claim, and VMware may, in its discretion, either provide such interoperability information to You, impose reasonable conditions, including a reasonable fee, on such use of the Software, or offer to provide alternatives to ensure that VMware's proprietary rights in the Software are protected and to reduce any adverse impact on VMware's proprietary rights.

3.3 Ownership. The Software and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Software and Documentation shall be limited to those expressly granted in this EULA and any applicable Order. No other rights with respect to the Software or any related Intellectual Property Rights are implied. You are not authorized to use (and shall not permit any third party to use) the Software, Documentation or any portion thereof except as expressly authorized by this EULA or the applicable Order.

3.4 Guest Operating Systems. Certain Software allows Guest Operating Systems and application programs to run on a computer system. You acknowledge that You are responsible for obtaining and complying with any licenses necessary to operate any such third-party software.

4. ORDER. Your Order is subject to this EULA. No Orders are binding on VMware until accepted by VMware. Orders for Software are deemed to be accepted upon VMware's delivery of the Software included in such Order. Orders issued to VMware do not have to be signed to be valid and enforceable.

5. AUDIT RIGHTS.

5.1 Records. You will, during the License Term for any Software licenses acquired under this EULA (and for a period of two (2) years from the expiration of the applicable License Term), maintain accurate records of your use of the Software sufficient to demonstrate Your compliance with the terms of this EULA and all Orders.

5.2 Audit Rights. During the period in which the You are obligated to maintain such records, VMware, or its third party auditor, may, upon reasonable notice to You, audit such records to verify that You have (a) used the Software solely in the manner authorized herein; (b) paid all applicable license fees; and (c) otherwise complied with the terms of this EULA and all Orders. VMware may conduct no more than one (1) audit in any twelve (12) month period. Audits will be conducted during normal business hours and VMware will use commercially reasonable efforts to minimize the disruption of Your normal business activities. VMware, and any third-party auditor, shall not have physical access to Your computing devices in connection with any such audit, without Your prior written consent. You will reasonably cooperate with VMware and/or its third-party auditor and will promptly pay directly to VMware any underpayments revealed by such audit. You will promptly reimburse VMware for all reasonable costs and expenses incurred by VMware for such audit if: (i) such audit reveals an underpayment by You of more than five percent (5%) of the fees payable by You to VMware for the period audited, or (ii) such audit reveals You have materially failed to maintain accurate records of Your use of the Software.

6. SUPPORT AND SUBSCRIPTION SERVICES. Except as expressly specified in the Product Guide, VMware does not provide any support or subscription services for the Software under this EULA. You have no rights to any updates, upgrades or extensions or enhancements to the Software developed by VMware unless you separately purchase VMware support or subscription services. These support or subscription services are subject to the Services Terms.

7. WARRANTIES.

7.1 Software Warranty. VMware warrants to You that the Software will, for a period of ninety (90) days following delivery ("**Warranty Period**"), substantially conform to the applicable Documentation, provided that the Software (a) has been properly installed and used at all times and in accordance with the applicable Documentation; and (b) has not been modified or added to by persons other than VMware or its authorized representative. VMware will, at its own expense and as its sole obligation and Your exclusive remedy for any breach of the foregoing warranty, either replace the applicable Software or correct any reproducible error in the Software reported to VMware by You in writing during the Warranty Period. If VMware determines that it is unable to correct the error or replace the Software, VMware will refund to You all License fees actually paid by You, in which case the License for the applicable Software and Your right to use such Software will terminate.

7.2 Disclaimer of Warranties. THE EXPRESS WARRANTY IN SECTION 7.1 ABOVE IS IN LIEU OF AND, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS LICENSORS DISCLAIM, ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE) REGARDING OR RELATING TO THE SOFTWARE, THE DOCUMENTATION, OR ANY MATERIALS FURNISHED OR PROVIDED TO YOU UNDER THIS EULA. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT THE SOFTWARE WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

8. INTELLECTUAL PROPERTY INDEMNIFICATION.

8.1 Defense and Indemnification. Subject to the remainder of this Section 8, VMware shall defend You against any third party claim that the Software infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that such misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) the People's Republic of China, to the extent that such countries are part of the Territory for the License ("**Infringement Claim**") and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement; provided that You: (i) promptly provide VMware with notice of such Infringement Claim; (ii) allow VMware sole control over the defense thereof and related settlement negotiation; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware.

8.2 Remedies. Should the Software become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense either: (a) procure the rights necessary for You to make continued use of the affected Software in accordance with this EULA; (b) replace or modify the affected Software to make it non-infringing; or (c) terminate the License to the affected Software and discontinue the related support services, and, upon Your certified deletion of the affected Software, refund: (i) the fees paid by You for the License to the affected Software, less straight-line depreciation over a three (3) year useful life beginning on the date such Software was delivered; and (ii) any pre-paid service fee attributable to related support services to be delivered after the date such service is stopped. Nothing in this Section 8.2 shall limit VMware's obligation under Section 8.1 to defend and indemnify You, provided that You replace the allegedly infringing Software upon VMware's making alternate Software available to You and/or You discontinue using the allegedly infringing Software upon receiving VMware's notice terminating the affected License.

8.3 Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 8 or otherwise with respect to any claim based on: (a) a combination of Software with non-VMware products (other than non-VMware products that are listed on the Order and used in

an unmodified form); (b) use for a purpose or in a manner for which the Software was not designed; (c) use of any older version of the Software when use of a newer VMware revision would have avoided the infringement; (d) any modification to the Software made without VMware's express written approval; (e) any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by VMware into Software listed on VMware's commercial price list; (f) any claim that relates to Linux or Android open source software, even when it has been embedded into or distributed with the Software or (g) any Software provided on a no charge, beta or evaluation basis. THIS SECTION 8 STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.

9. LIMITATION OF LIABILITY.

9.1 Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS EULA WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE LICENSE FEES YOU PAID FOR THE SOFTWARE, IF ANY. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

9.2 Further Limitations. VMware's licensors shall have no liability of any kind under this EULA and VMware's liability with respect to any third party software embedded in the Software shall be subject to Section 9.1. You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises.

10. TERMINATION.

10.1 License Term. This EULA will terminate in its entirety upon the termination of the License Term, unless terminated earlier under this Section 10.

10.2 Termination for Breach. VMware may terminate this EULA in its entirety effective immediately upon written notice to You if: (a) You breach any provision in Section 3 and do not cure the breach within ten (10) days after receiving written notice thereof from VMware; (b) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; (c) You breach any other provision of this

EULA and don't not cure the breach within thirty (30) days after receiving written notice thereof from VMware; or (d) You commit a material breach that is not capable of being cured.

10.3 Termination for Insolvency. VMware may terminate this EULA in its entirety effective immediately upon written notice to You if You: (a) terminate or suspend your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding.

10.4 Effect of Termination. If VMware terminates this EULA under this Section 10: (a) all Licensed rights to all Software granted to You under this EULA will immediately cease to exist; and (b) You must promptly discontinue all use of all Software, and (destroy all copies of the Software and all License Key(s)) and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Sections 1 (Definitions), 2.6 (Open Source Software), 3 (Restrictions; Ownership), 5.1 (Records), 5.2 (Audit Rights), 7.2 (Disclaimer of Warranties), 9 (Limitation of Liability), 10 (Termination), 11 (Confidential Information) and 12 (General) will any survive termination of this EULA.

11. CONFIDENTIAL INFORMATION.

11.1 Definition. "Confidential Information" means information or materials provided by one party ("Discloser") to the other party ("Recipient") which are in tangible form and labeled "confidential" or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) License Keys; (b) information regarding VMware's pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Software.

11.2 Protection. Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this EULA; or (b) in connection with the parties' ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by the EULA, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for purposes of the EULA and who are under a duty of confidentiality no less restrictive than Recipient's duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

11.3 Exceptions. Recipient's obligations under Section 11.2 with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality

restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser's Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser's request and expense, in any lawful action to contest or limit the scope of such required disclosure.

11.4 Data Privacy. You agree that VMware may process technical and related information about Your use of the Software which may include internet protocol address, hardware identification, operating system, application software, peripheral hardware, and non-personally identifiable Software usage statistics to facilitate the provisioning of updates, support, invoicing or online services and may transfer such information to other companies in the VMware worldwide group of companies from time to time. To the extent that this information constitutes personal data, VMware shall be the controller of such personal data. To the extent that it acts as a controller, each party shall comply at all times with its obligations under the local legislation applicable in the Territory for the protection of individuals with regard to the processing of personal data. Collected data is subject to VMware's Privacy Policy at <http://www.vmware.com/help/privacy.html>.

12. GENERAL.

12.1 Assignment. This EULA and any Orders, and any of Your rights or obligations thereunder, may not be assigned, subcontracted or transferred by You, in whole or in part, whether voluntary, by operation of contract, law or otherwise, without the prior written consent of VMware. Any attempted assignment or transfer in violation of the foregoing will be null and void. Subject to the foregoing, this EULA will be binding upon and will inure to the benefit of the parties and their respective successors and assigns.

12.2 Notices. Any notice delivered by VMware to You under this EULA will be delivered via mail, email or fax.

12.3 Waiver. The waiver of a breach of any provision of this EULA shall not constitute a waiver of any other provision or any subsequent breach.

12.4 Severability. If any provision of this EULA is held to be illegal, invalid or unenforceable, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this EULA will remain in full force and effect.

12.5 Compliance with Laws; Export Control; Government Regulations. Each party shall comply with all laws applicable to the actions contemplated by this EULA. You acknowledge that the Software is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) you are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) you will not permit the Software to be used for, any purposes prohibited by law, including, any

prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. The Software and accompanying documentation are deemed to be “commercial computer software” and “commercial computer software documentation”, respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and documentation by the U.S. Government shall be governed solely by the terms and conditions of this EULA.

12.6 Construction. The headings of sections of this EULA are for convenience and are not to be used in interpreting this EULA. As used in this EULA, the word ‘including’ means “including but not limited to.”

12.7 Governing Law. This EULA is governed by the laws of the State of California, United States of America, unless mandated by other law. The United Nations Convention for the International Sale of Goods shall not apply.

12.8 Third Party Rights. Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.

12.9 Product Guide. In addition to the above sections, Your use of the Software is subject to the terms and conditions of the Product Guide, which is incorporated herein by reference.

12.10 Order of Precedence. In the event of conflict or inconsistency among the Product Guide, this EULA and the Order, the following order of precedence shall apply: (a) the Product Guide, (b) this EULA and (c) the Order. With respect to any inconsistency between this EULA and an Order, the terms of this EULA shall supersede and control over any conflicting or additional terms and conditions of any Order, acknowledgement or confirmation or other document issued by You, unless the parties execute a written agreement expressly indicating: (i) that such Order shall modify this EULA; or (ii) that the terms of such Order shall supersede and control in the event of any inconsistency.

12.11 Entire Agreement. This EULA, including accepted Orders and any amendments hereto, and the Product Guide contain the entire agreement of the parties with respect to the subject matter of this EULA and supersede all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This EULA may be amended only in writing signed by authorized representatives of both parties.

12.12 Contact Information. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America. If You have any questions concerning this EULA, please send an email to info@vmware.com.

- See more at:

http://www.vmware.com/download/eula/esxi50_eula.html#sthash.OedwR8GU.dpuf

EXHIBIT L
REQUEST FOR PROPOSALS (RFP)
FOR
MBIS SOLUTION

INCORPORATED BY REFERENCE

EXHIBIT M
CONTRACTOR'S PROPOSAL
FOR
MBIS SOLUTION

INCORPORATED BY REFERENCE